13 MAY 96

Defense Software Repository System

Functional Description for the DSRS

U. S. Department Of Defense
Defense Information Systems Agency
Joint Interoperability and Engineering Organization
Center for Computer Systems Engineering
Software Reuse Program

Submit comments and suggested improvements to:

Center for Operational Support
Software Reuse Program
Room 632
5600 Columbia Pike
Falls Church, VA 22041

1st Edition, March 1993
2nd Edition, June 1993
Change pages issued December 1993
Change pages issued January 1994
3rd Edition, February 1994
4th Edition, June 1994
5th Edition, September 1994
6th Edition, June 1995
7th Edition, September 1995
8th Edition, May 1996

Document No:	PD204.7:13-MAY-96
Contract No:	DCA100-93-D-0071
Delivery Order:	DO75
CDRL No:	A0005

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

SECTION 1
GENERAL

1.1 PURPOSE OF THE FUNCTIONAL DESCRIPTION. This *Functional Description for the DSRS* is written to provide:

a. System requirements that will serve as a basis for mutual understanding between the user and the developer;

b. Information on functional requirements, design considerations, and user impacts; and

c. A basis for development of system tests.

1.2 PROJECT REFERENCES. The Defense Software Repository System (DSRS) is an automated repository designed primarily to assist users in the reuse of assets. The project sponsor is the Defense Information Systems Agency/Joint Interoperability and Engineering Organization/ Center for Operational Support (DISA/JIEO/CFOS). The DSRS is operational at the DISA/JIEO/CFOS Software Reuse Program (SRP) site in Falls Church, VA, and at other remote sites designated by the SRP.

The following is a list of project references used during development of this Functional Description (FD). Unless otherwise indicated, all references are UNCLASSIFIED:

a. **Project Request or Other Initiation Documentation**

(1) *DSRS Interoperation Plan*, December 3, 1994.

(2) *DSRS/ASSET/CARDS Library Interoperation*, Final, Engineering Working Group, July 1993.

b. **Risk Analysis Studies**

A formal quantitative risk analysis for the DSRS has been conducted for DISA's implementation of the DSRS.

(1) *Risk Assessment of Defense Software Repository System* (DSRS), Center for Information Systems Security, August 1994.

(2) *DSRS Security Test and Evaluation* (STE), Center for Information Systems Security, October 1994.

c. **Other Pertinent Manuals or Documents**

(1) The DSRS system documentation follows the format standards of DoD-STD-7935A and consists of the following: Functional Description, Database Specification, System Specification, User Manual (for Windows and X/Motif), Librarian Manual (for Windows), Maintenance Manual, System Administration Manual, Implementation Procedures, Test Plan, and Test Analysis Report.

(2) The DSRS security documentation consists of the following: Trusted Facility Manual, System Security Plan, Contingency Action Plan, and Security Features User Guide (included in the User Manuals).

d. **Standards or Reference Documentation**

(1) Programming Conventions

(a) X/Motif-based DSRS

This version will be written in ANSI C and C++. Pro*C is used to generate low-level calls to the database.

(b) Windows-based DSRS

This version will be written in Visual Basic using SQL*Net (Librarian only) and TCP/IP messages to retrieve information from the database.

(2) DoD Standards and References

The following references are used for the development of the system and its documentation:

(a) DoD-STD-7935A, *Military Standard - DoD Automated Information Systems (AIS) Documentation Standards,* 31 October 1988.

(b) *Technical Reference Model for Corporate Information Management, Version 1.1,* 27 November 1991.

(c) DoD Directive 5200.28, *Security Requirements for Automated Data Process (ADP) Systems,* 21 March 1988.

(d) DoD Directive 5200.1-R, *Information Security Program Regulations,* June 1986.

(e) CSC-STD-004-85, *Guidance for Applying the Department of Defense Trusted Computer Evaluation Criteria in Specific Environments,* (also known as "The Yellow Book"), 25 June 1985.

(f) DoD Directive 5200.28-STD, *Department of Defense Trusted Computer System Evaluation Criteria*, (also known as "The Orange Book"), 26 December 1985.

(g) DISA Instruction 6030-230-19, *Security Requirements for Automated Information Systems* (AIS), August 1991.

(3) System Documentation

(a) *System and Network Administration*, Sun Microsystems, Inc., 1990.

(b) *Microsoft Windows User's Guide*, Microsoft Corporation, 1993.

(c) *Microsoft MS-DOS User's Guide*, Microsoft Corporation, 1994.

1.3 ACRONYMS AND TERMS.

1.3.1 Acronyms.

ADP Automated Data Processing

AIS Automated Information System

ANSI American National Standards Institute

ARF Account Request Form

ASSET Asset Source for Software Engineering Technology

CARDS Comprehensive Approach to Reusable Defense Software

CFSW Center for Software

COTS Commercial-Off-the-Shelf

DAA Designated Approving Authority

DBMS Database Management System

DDN Defense Data Network

DISA	Defense Information Systems Agency
DOD	Department of Defense
DSRS	Defense Software Repository System
FD	Functional Description
FTP	File Transfer Protocol
HW	Hardware
IP	Internet Protocol
JIEO	Joint Interoperability and Engineering Organization
KB	Kilobyte
MB	Megabyte
MODEM	Modulator/Demodulator
MS	Microsoft
PC	Personal Computer
PPP	Point-to-Point Protocol
RA	Reusable Asset
SLIP	Serial Line Internet Protocol
SOP	Standing Operating Procedures
SRP	Software Reuse Program
STE	Security Test and Evaluation
SW	Software
TCB	Trusted Computing Base

TCP	Transport Control Protocol
UBS	Unclassified but Sensitive
UID	Unique Identifier
WWW	World Wide Web

1.3.2 Terms.

Asset	See entry below for RA.
Candidate RAs	A collection of assets that have been identified by searching the DSRS catalog.
Catalog	A collection of assets and their related information.
Classification Scheme	The model applied to assets to organize them for searches.
Client	The software operating on a user's PC that communicates with the software operating at the server where the DSRS repository resides.
Cooperating DSRS Site	A site that chooses to make its assets available for extraction by other DSRS sites.
Descriptor	A descriptor consists of a domain, facet, and facet term.
Domain	The major category of assets to search.
Ethernet	The predominant form of local area network technology used with TCP/IP.
Extract	A function available in the DSRS software that allows the user to obtain desired RAs.
Facet	Facets are properties an RA may have. They represent different ways of looking at an asset; i.e., "aspects" or "views".
Facet Term	The facet terms describing an RA can be thought of as keywords describing the asset, except that the facet terms are a much more structured and precise method of identification.
Foreign Site	Non-DSRS remote site that is interoperable with the DSRS.
Internet	A worldwide network of networks connecting computers at universities, research laboratories, and commercial and Government sites.

Interoperability The concept of allowing multiple installations of the DSRS to communicate with each other and other reuse libraries, sharing catalogs and exchanging RAs.

Librarian (1) The individual who maintains the DSRS catalog.

(2) A type of user who functions as a librarian and has a subset of the rights to perform any action on the DSRS.

Local Site The site of the local repository.

Metric A characteristic of an RA that is assigned a numeric value.

RA Reusable Asset. An asset that has potential to be used more than once. Types of reusable assets include architectures, designs, software, test suites, software tools, document type definitions, documents and templates, and reuse library support items.

RA State There are three RA States: Certified, Active and Archived. Only Active RAs are available to be candidate RAs. Certified RAs are being evaluated through certification procedures prior to being made available to users. Archived RAs have been identified as obsolete, but archiving is safer than deleting. The files of Archived RAs still appear on the system.

Remote Site DSRS site that is interoperable with the DSRS.

Repository The database entries and all the associated files that the database references.

Server The machine where the DSRS resides and the DSRS software operating there that communicates with the client software operating on the user's PC.

Site An installation of the DSRS server software.

Supervisor A type of user who functions as a librarian and has the rights to perform any action on the DSRS.

System Administrator An individual who maintains: (1) the computer system on which DSRS is operating, and (2) the tools that are required for the execution of the DSRS, such as the ORACLE database.

Telnet A TCP/IP application for remote terminal emulation.

UID Unique Identifier. An identifier for the RA that supports interaction with foreign (non-DSRS) sites.

Usage Log Log of RAs that have been extracted by programmer-level users. The values of this log may be viewed in the DSRS Librarian tool.

SECTION 2
SYSTEM SUMMARY

2.1 BACKGROUND. The DSRS is the product of an evolution of software developed under the DISA/JIEO/CFSW Software Reuse Program. It is an automated repository designed to support a strategy of asset reuse. Reuse is the application of previously developed assets to a new system or an expansion and/or enhancement of an existing system. A software reuse program may take the following approach to implement this strategy:

a. Identify reuse opportunities through avenues such as domain analysis;

b. Provide users with a facility to find, evaluate, and acquire reusable assets;

c. Provide asset configuration management and quality assurance;

d. Establish policies and procedures; and

e. Provide reuse training and support.

The DSRS supports this strategy by providing a facility for finding, evaluating, and storing reusable assets. Additionally, the DSRS supports asset configuration management.

The DSRS supports the distribution of reusable assets through two automated tools:

a. The DSRS Librarian tool is a mechanism of the software reuse program which provides for:

   (1) Managing the catalog of assets, and

   (2) Reports on usage of the system.

b. The DSRS User tool is outside the scope of the software reuse program and provides for:

   (1) Users to request and obtain assets.

2.2 OBJECTIVES. The overall objective of the SRP is to promote the application of reuse to reduce the cost associated with system development. The DSRS will automate access to reusable assets. The DSRS will perform the following functions:

a. Provide users with a repository system in which multiple users can simultaneously search for, evaluate, and acquire reusable assets;

b. Provide a tool to perform various maintenance activities for the repository of reusable assets; and

c. Provide the capability to interact with other DSRS sites and other interoperable repositories to increase the availability of reusable assets.

2.3 EXISTING METHODS AND PROCEDURES. Reuse not only applies to source code, but also to other products of the development life-cycle, which may include: requirements documentation, system specifications, user manuals, design documentation, test suites, and any information to support development of software. Currently, asset reuse is limited to an individual's knowledge of ad hoc, localized methodologies that are customarily project specific, thereby discouraging the transfer of technology from one project or department to another.

2.4 PROPOSED METHODS AND PROCEDURES. The system will provide a repository in which multiple users can simultaneously search for, evaluate, and acquire reusable assets and in which the DSRS support staff can perform various maintenance activities for the repository of assets.

The DSRS will provide a structured querying mechanism with a user-friendly interface. Figure 2-1 displays the basic DSRS architecture, which lists each executable and the mapping of each executable to the user interface, DSRS software, Database Management System (DBMS), and the operating system.

The User Tool will be implemented on a Sun/UNIX workstation to support a Motif-based interface; and implemented for a PC/Windows workstation to support a Windows-based interface. The User Tool functionality will be consistent between each interface supported, unless limited by the host environment.

The Librarian Tool will be implemented for a PC/Windows workstation to support a Windows-based interface.

The DSRS Server will be built on a relational database, which organizes information about the reusable assets. The reusable asset files (including the actual asset, an abstract file, and document files) will be stored in the underlying file system provided by the operating system software and will be transparent to the user.

DSRS Applications	User		Librarian
Client Executables	DSRS	DSRS60	DSRSLIB
Client HW/OS*	PC/DOS	Sun/UNIX	PC/DOS
User Interface	MS-Windows	X/Motif	MS-Windows
DBMS	Oracle/Access	Oracle/MSQL	Oracle
Server Executables	pc_server or pc_server.sol23 and dsrs_server or dsrs_server.sol23		lib_server or lib_server.sol23
Server HW/OS*	Sun/UNIX		

* Refer to Section 5.2 for environment specifics.

Figure 2-1. Basic DSRS Architecture

2.4.1 User Tool. Figure 2-2 shows the User Tool process. The following paragraphs briefly discuss, at a high level, each of the major functions.

Figure 2-2. User Tool Process Figure 2-2. User Tool Process

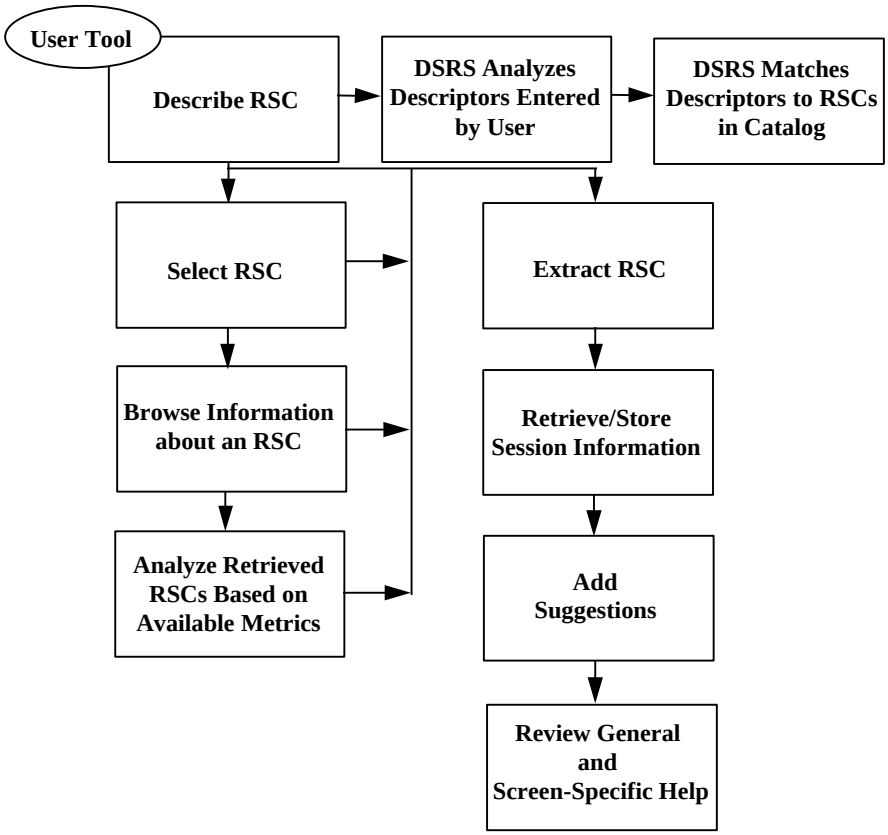


Figure 2-2. User Tool Process

2.4.1.1 Search Mechanisms. The user's main interaction with the system will be searching for an RA. The user, having determined in advance the objective of the search, will use the following types of search mechanisms to help build a Candidate List of RAs:

a. **List RA IDs.** The system will create a list of candidate RAs based on the domain(s) selected by the user and the RA ID or wildcard RA ID entered by the user.

b. **List RA Names.** The system will create a list of candidate RAs based on the domain(s) selected by the user and the RA Name or wildcard RA Name entered by the user.

c. **Find Keywords.** The system will create a list of candidate RAs based on the domain(s) selected by the user to be searched and the keywords entered by the user. The system will search the repository for RAs in which the keywords can be found in the abstract files.

d. **Catalog Indexes (WWW).** The system will display the indexed catalog of RAs via a WWW browser previously specified by the user.

2.4.1.2 Browse RA Information. The user may choose to browse information about a candidate RA. Such information will include the RA file list (including abstract, source, document, or problem report files), metrics, and related RAs. The user will also be able to view information stored on a WWW page about the selected RA.

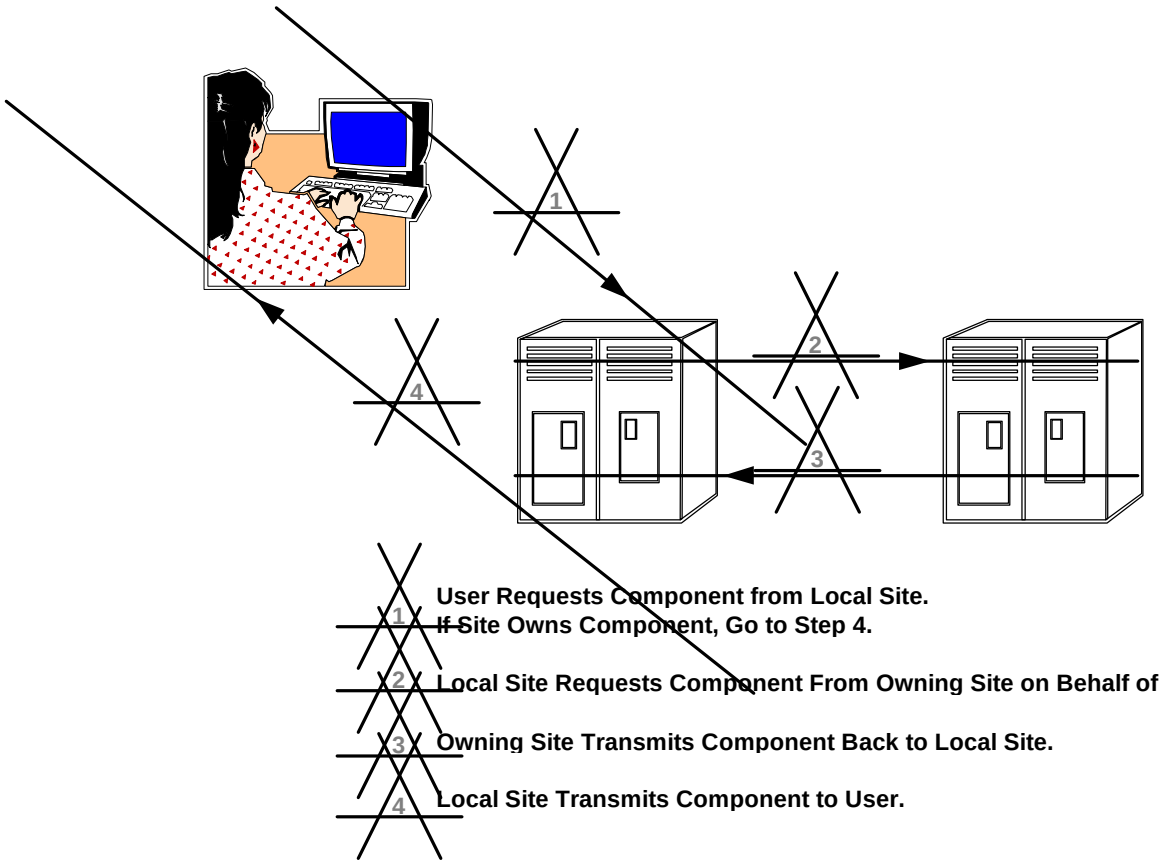
2.4.1.3 Tools. The system will provide the capability to display a list of metrics, analyze the candidate RAs based on a metric, clear the local catalog information, and sort the Candidate List.

2.4.1.3.1 Analyze. The user may also choose to analyze the list of retrieved RAs based on available metrics and sort them according to the available options. The sort may be in ascending or descending order or none (as it appears in the candidate list).

2.4.1.3.2 Clear Local Catalog. The user may choose to clear the information stored in the local database.

2.4.1.3.3 Sort List. The user may choose to sort the list of candidate RAs based on the RA ID or RA Name.

2.4.1.4 Extract RAs. The user may select multiple RAs from the Candidate List to be extracted. Once the user selects the RAs, the system will identify any RAs related to each RA selected. Depending on the user's access rights, the system will also allow extraction of the related RAs. Users may extract assets interactively from the local site, remote DSRS sites, or foreign sites (other interoperable repositories) via the TCP/IP Asset Transfer Interface. The extraction process is illustrated in Figure 2-3.



Users' access to assets will be determined by the assignment of group identifiers. Asset access will be managed by the Librarian assigning group identifiers to site IDs, user IDs, and RA IDs. A group ID will be a tag identifying an abstract collection of sites, users, and assets and conveying certain rights and privileges to the members of that collection. Asset access for groups is depicted in Figure 2-4.

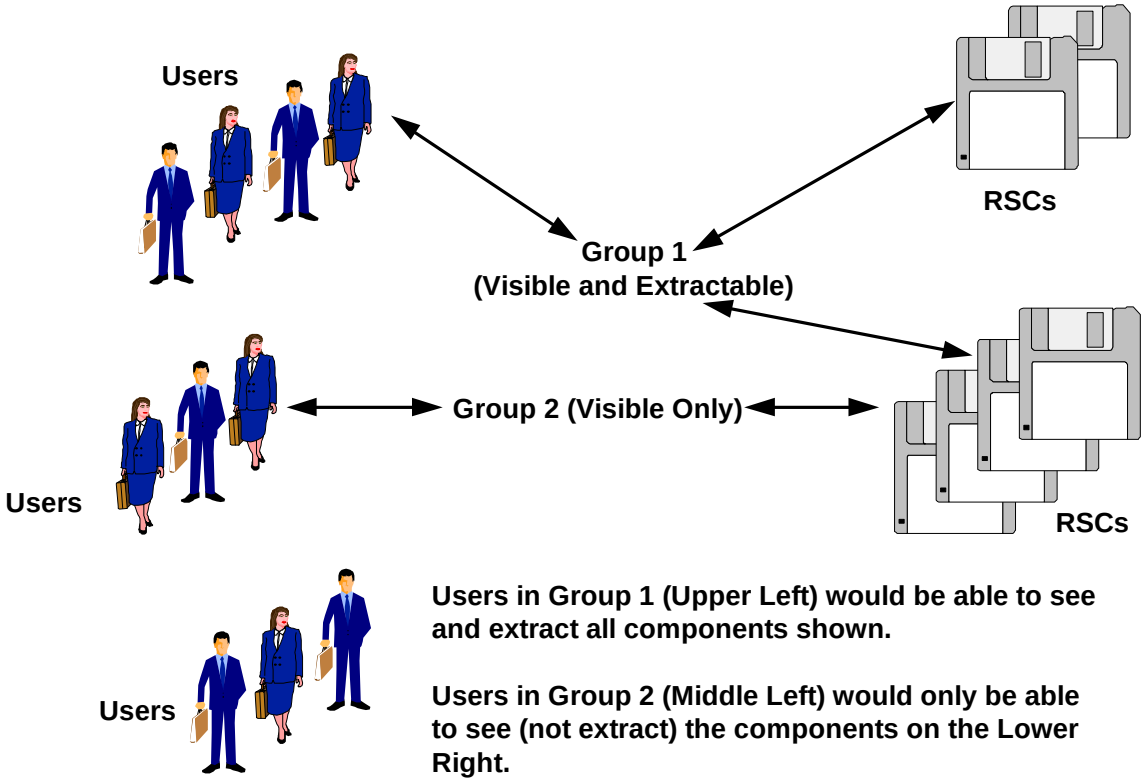


Figure 2-4. Asset Access for Groups

2.4.1.5 Sessions. The user will be able to retrieve and save session information containing the RA ID and RA Names in the Candidate List and the domains used to create the Candidate List.

2.4.1.6 Options. The system will allow users to set options for the following:

a. **Change Password**. The system will allow users to change their password.

b. **Preferences.** The system will allow users to select a default domain (used when searching) and the default text browser (used when viewing text RA files).

c. **Network.** The system will allow users to enter network configuration information to be used when connecting to the DSRS server. The system will also allow users to test their network communication to the server.

d. **WWW.** The system will allow users to enter configuration information for the WWW browser to be used with functions that launch a WWW browser.

2.4.1.7 Help. The system will provide on-line help, a tutorial for beginner users, and a suggestion form. The system will provide the user with the capability to search the on-line help by selecting from a list of available topics. The system will provide users with the capability to submit comments and questions to the Librarians via the on-line suggestion form.

2.4.2 Librarian Tool. The Supervisor/Librarian for the DSRS will be responsible for maintaining the assets in the repository and the information that supports the operation of the system. Figure 2-5 shows the Librarian Tool process. The following paragraphs briefly discuss, at a high level, each of the major functions.

2.4.2.1 RAs. The Supervisor/Librarian will be able to maintain the RAs and RA information in the local catalog. The RA information will include RA Classification, RA Metrics, relationships with other RAs, and RA Files.

2.4.2.2 Groups. The Supervisor/Librarian will be able to maintain group information and group assignments for the local, remote and foreign sites. Groups will be used to control access to assets of the local repository to local users by designating users, sites, and RAs collectively. Groups will be used to control access to assets of the local repository to remote and foreign site users by designating sites. The remote or foreign site will designate with users will be authorized to access the group of assets.

2.4.2.3 Users. The Supervisor/Librarian will be able to maintain user information and assignments for local users. User IDs and passwords will be used to validate and control access to the system.

2.4.2.4 Sites. The Supervisor/Librarian will be able to maintain the information for local and remote DSRS sites, and for foreign sites (other interoperable repositories). Site IDs are used to help formulate and validate RA IDs and will be used to validate sites to determine access rights to Ras.

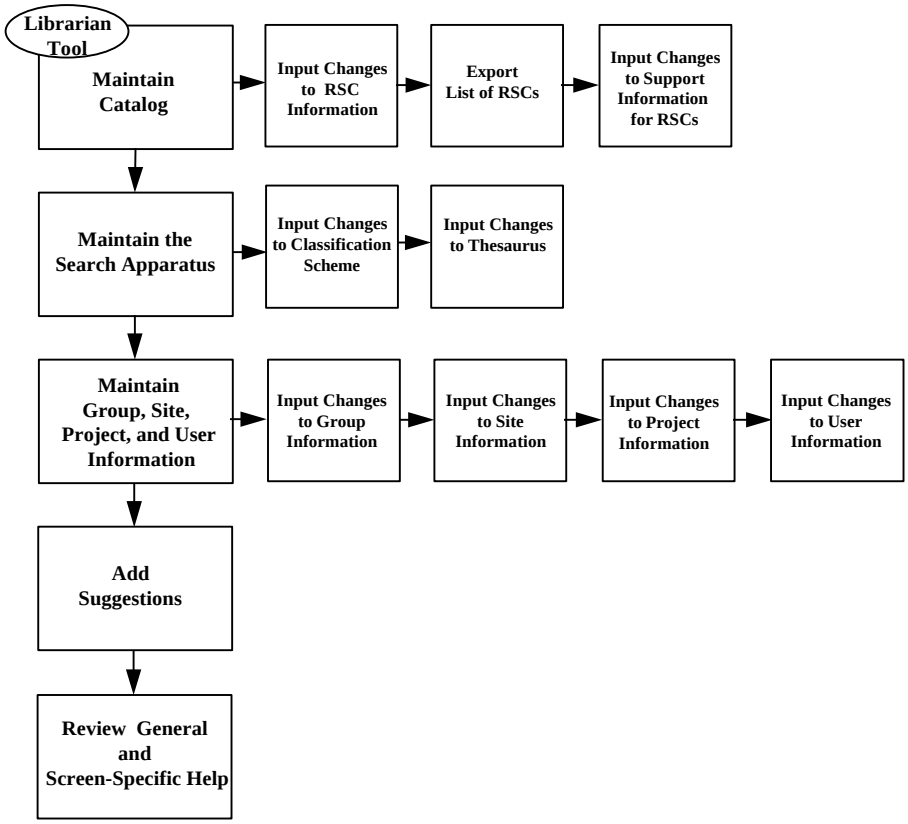


Figure 2-5. Librarian Tool Process

2.4.2.5 Classification Scheme. The Supervisor/Librarian will be able to maintain the classification scheme that will be used to describe the attributes of an RA. The classification scheme will be composed of domains, facets, and facet terms.

2.4.2.6 Metrics. The Supervisor/Librarian will be able to maintain the types of metrics indigenous to the local site.

2.4.2.7 Relationships. The Supervisor/Librarian will be able to maintain the types of relationships that can be used when entering related RAs.

2.4.2.8 Logs. The Supervisor/Librarian will be able to maintain the entries in the Usage Log.

2.4.2.9 Import. The Supervisor/Librarian will be able to read RA information contained in an export file (created at another DSRS) and write the information to the local catalog (the local database). The Import function will verify that the file is in the correct DSRS export file format.

2.4.2.10 Export. The Supervisor/Librarian will be able to submit assets to other DSRS sites via the Export function. The Export function will create an export file containing RAs and associated information to be imported into another DSRS catalog. The Export function will also create index files to be imported into other interoperable repositories (foreign sites).

2.4.2.11 Reports. The Supervisor/Librarian will have the capability to generate predefined or customized reports on the data stored in the database.

2.4.2.12 Options. The Supervisor/Librarian will have the capability to enter configuration information for the server's host name and database.

2.4.2.13 Help. The system will provide on-line help, a tutorial for beginner users, and a suggestion form. The system will provide the user with the capability to search the on-line help by selecting from a list of available topics. The system will provide users with the capability to submit comments and questions to the Librarian via an on-line suggestion form.

2.4.3 Server. The Server will process the following:

a. **Authentication Requests.** The server will authenticate users logging in from the DSRS User Tool and the DSRS Librarian Tool.

b. **Catalog Requests.** The server will process catalog update requests from the DSRS User Tool and the DSRS Librarian Tool. These requests will be used to facilitate consistency between the server database and client cache database.

c. **File Transfer Requests.** The server will process file transfer requests from the DSRS User Tool, remote DSRS sites, and foreign sites (other interoperable

repositories). Figure 2-3 illustrates the processing that occurs when files are transferred between servers and a local client.

SECTION 3
DETAILED CHARACTERISTICS

3.1 SPECIFIC PERFORMANCE REQUIREMENTS. The system will meet the following specific performance requirements:

a. The system will interoperate with remote DSRS sites and foreign sites (other interoperable repositories) via electronic data transfers.

b. Catalog updates that occur as part of the import/export process will maintain catalog integrity. Catalog integrity will be maintained by ensuring that all incoming updates containing information compatible with the receiving site's catalog are accurately loaded without omission. "Compatible" means the description of the asset is valid according to the receiving site's classification scheme.

c. Depending on the type of user and access authority granted, the system will restrict access to processes and data.

d. The system will support interactive editing of input transactions on-line and will report errors for correction during input.

e. The system will immediately update the database with transactions before leading the user to the next transaction.

3.1.1 User Interface Features.

3.1.1.1 Interactive Response. The DSRS is structured and menu-driven. "Hot key" features will allow the user to execute menu items through short key sequences. The system will provide on-screen instructions for the user as follows:

a. An explanation will be provided on how to exit each screen, what keys to press for Help, and what commands are appropriate to the task being performed. These will be available either from a "status line" or from a pull-down or pop-up menu.

b. The user interface will be sufficiently informative that an experienced user should not have to rely on printed documents, such as a user manual, to execute the primary functions of the DSRS.

c. The system will remain in contact with the user by displaying the mouse pointer or cursor at all times or by acknowledging that the system is performing some function during delays.

d. Since the system will be interactive, it will acknowledge every keystroke by "echoing" immediately on the screen.

e. The system will query the user for confirmation when an unrecoverable change will take place, such as a deletion of existing data.

f. The system will advise the user when a change has taken place, such as an addition or update to existing data.

3.1.1.2 Help Text and Error Messages. Help text and error messages will be phrased simply, using an active-voice sentence with few technical terms. These messages will avoid emotional or accusatory verbiage, such as "error", "abort", or "crash", by directing the user with the correct input or command. The help text and error handling messages will be context-sensitive to provide direct assistance based on the task being performed.

3.1.1.3 Display Layout. The screen layout throughout the system will be consistent and follow a "windowing" style and format. Where possible, screens will utilize windowing features to maximize both functionality and intuitiveness. Consistency between the implementations of the user interfaces will be maintained wherever possible.

3.1.1.4 Command Entry. Methods of command entry may vary between the character and graphical implementations of the user interface, depending on the type of terminal or terminal emulation used. The command style will be consistent throughout each interface, with alternatives available whenever possible to provide easy navigation of menus and screens. In addition, the following functionality will aid command entry:

a. Fill-in-the-blank fields;

b. Non-case sensitive alphabetic input;

c. Backspacing in data fields, returning to data fields, canceling the input, etc., before exiting a data input screen;

d. Verification of data type, values, ranges, etc., for each data field;

e. Consistent function key usage;

f. Positive confirmation before destructive commands; and

g. Removal of leading blanks from all user-entered data fields before processing by the system.

3.1.1.5 Menus. Menus will provide user guidance for choosing between functional options or navigating throughout the system. The user will be able to return to a previous menu, move to the top of the menu tree, or leave the system from appropriate menus.

3.1.1.6 User Error Handling. The system will notify the user when an invalid entry has been entered for a given field and will permit the user to correct errors before leaving the function being performed.

3.1.2. Accuracy and Validity. The following items represent the general accuracy and validity performance requirements:

a. The system will verify all interactive transactions for valid codes in each data element, consistency with other data elements in the transaction, and consistency with the data in the database. When an error occurs during a data entry transaction, the system will notify the user and allow correction of the appropriate fields without having to re-key every entry.

b. The system will verify all batch transactions for valid codes in each data element, consistency with other data elements in the transaction, and consistency with the data in the database. If an error occurs during import, the system will write error information to a log.

c. The system will not leave incomplete transactions in the database as a result of a system malfunction.

d. The system will maintain data and produce reports based on the information stored in the database.

3.1.3 Timing. The DSRS will be developed to minimize response time as much as possible, based on the underlying computer system, number of records in the database, and complexity of database relations. Enhancements to the system will maintain or improve system response time.

3.1.4 Capacity Limits. The capacity limits (e.g., number of database entries) will vary, depending on the size and complexity of the information being maintained. Refer to Section 5.1 of this document for specific information.

3.2 FUNCTIONAL AREA SYSTEM FUNCTIONS. This section further describes the processing activities within each functional area as introduced in Section 2.4. Each area is discussed, in general, in the following paragraphs. Section 4.2 enumerates all the capabilities of each identified functional area.

The DSRS provides a repository system in which multiple users can simultaneously search for reusable software assets and in which a Librarian can perform various maintenance activities for the database of assets. Assets may be extracted in real time by one site from another site. To implement these functions, the DSRS can be divided into the following system functions:

3.2.1 User Interaction.

a. Search Mechanisms
   (1) List RA IDs
   (2) List RA Names
   (3) Find Keywords
   (4) Catalog Indexes (WWW)
b. Browse information about an RA
c. Tools
   (1) Analyze retrieved RAs based on available metrics
   (2) Clear local database
   (3) Sort Candidate List by RA ID or RA Name
d. Extract local, remote, or foreign RAs. The extraction of remote and foreign RAs will be managed and controlled by the TCP/IP Asset Transfer Interface
e. Provide storage and retrieval of session information
f. Provide options for preferences (defaults), network, and WWW configurations
g. Provide on-line help, suggestions, and tutorial

3.2.2 Librarian Interaction.

a. RAs
   (1) RA Information
   (2) RA Classification
   (3) Related RAs
   (4) RA Metrics
   (5) RA Files
b. Group Information and Group Assignments
c. User Information and User Assignments
d. Site Information and Site Assignments
e. Classification Scheme
f. Metrics

g. Relationships
h. Logs
i. Provide Import of RAs
j. Create Export files
k. Reports
l. Provide option to set server configuration
m. Provide on-line help, tutorial, and suggestion form

3.2.3 Server Interaction.

a. Authentication Requests
b. Catalog Requests
c. File Transfer Requests

3.3 INPUTS AND OUTPUTS.

3.3.1 Inputs. The general inputs for the DSRS that are specified by each subschema consist of the following: RA Data, Classification Data, User Data, Access Control Data, and Tracking Data. Specific information for inputs may be found in the *Database Specification for the DSRS* document.

3.3.2 Outputs. The DSRS provides interactive views of the database and produces reports on demand. The reports produced by the system are identified in the *System Specification for the DSRS.*

The export function output consists of a file that will include all the associated information for each RA in the Group ID to be exported. This RA information may include: the abstract, classification, RA files, related RAs, and metric values. Specific contents of the export file are contained in paragraph 4.2.2.10 of this document.

3.4 DATABASE CHARACTERISTICS. Approximately 60 MB of space will store metadata for up to 1,500 RAs. Since the size of files associated with an RA varies significantly from asset to asset, estimation of the data storage requirements and growth rate would be inappropriate. Database characteristics and information on data elements are published in the *Database Specification for the DSRS.*

3.5 FAILURE CONTINGENCIES. In the event of system failure, the user will not lose more than the current search session and the Librarian will not lose more than one transaction. To assist the user in knowing when a session has been saved, the DSRS will present a confirmation message at the completion of saving the session. To assist the Librarian in knowing when a transaction has been completed, the DSRS will present a confirmation message at the completion of the transaction.

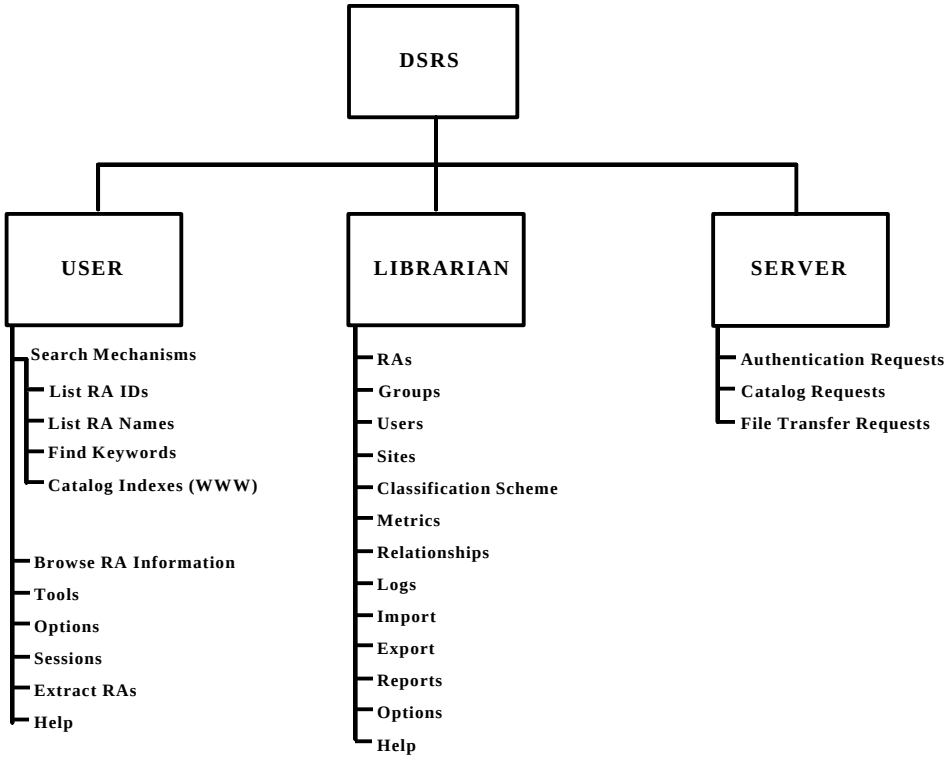
Each DSRS site will be responsible for computer hardware and software integrity and for coordinating appropriate contingency plans for operational failure. The System Administrator must maintain sufficient backups to assure minimal system losses in the case of system failure. Refer to the *System Administration Manual for the DSRS* for details on recovery/restart procedures.

There are no manual means to accomplish the DSRS requirements in the event DSRS is unavailable to the user. The user may refer to a hard copy of the librarian catalog or the WWW to review a list of available assets.

SECTION 4
DESIGN CONSIDERATIONS

4.1 SYSTEM DESCRIPTION. The system is designed to assist users in the reuse of assets. Given a description of the assets for which the user is searching (the user's formal description), the system identifies one or more suitable RAs from its catalog (which may include RAs defined by the local site as well as RAs from other DSRS sites, and other interoperable repositories) and supplies the necessary information so that the user may request the complete RA or selected RA files (source, manuals, documentation, testing material, etc.). To support this central function, the system maintains a catalog of available RAs and multiple search mechanisms to help the user locate and extract desired asset(s).

Figure 4-1 illustrates an organizational chart for DSRS that depicts the different system



functions for the User, Librarian, and Server.

4.2 SYSTEM FUNCTIONS. This section provides a detailed description of the system functions outlined in Section 3.2.

4.2.1 User Tool. The user's main interaction with the system will be searching for reusable assets. The user will have the option to build a new list of candidate RAs using the search mechanism or restore a session file with a list of previously built candidate RAs. The following fields will be displayed for each RA in the Candidate List:

a. **RA ID and Version.** The RA ID will be an 8-position alphanumeric identification assigned to each RA. The first two positions of the RA ID will indicate the site ID where the RA will be physically located. The RA ID will be automatically displayed by the system and will not be editable. The version is a numeric value.

b. **RA Name.** The RA Name will be displayed for each RA in the Candidate List and will not be editable.

c. **Total Size.** The total size in kilobytes (KB) up to 13-positions will be displayed for each RA in the Candidate List and will not be editable.

The number of RAs that the system will be capable of processing in the Candidate List will be determined by the available memory at runtime. The system will notify and not exit the user from the system when capacity limits are exceeded for displaying the metadata that comprise or is associated with the user's Candidate List. Once a Candidate List exists, the user will also have the option to browse descriptive information about each listed RA, analyze the RAs based on available metrics, extract the RAs, and save the Candidate List to a session file.

The user will have the option to double-click on any RA in the Candidate List to Browse the RA abstract, as described in paragraph 4.2.1.2.1.1.

4.2.1.1 Search Mechanisms. The user will be able to use the following search mechanisms to build a Candidate List: list RAs by wildcard RA ID, by wildcard RA Name, and based on keyword(s) entered. The user will be able to use multiple search mechanisms (as listed above) to build one Candidate List. When using multiple search mechanisms, the system will sort the Candidate List based on (1) the existing Candidate List; (2) any new RAs retrieved based on the search mechanism (any duplicates will be discarded); and (3) the Append and Replace options available within each search mechanism. Also, the user may view the WWW-based catalog index to locate potential RAs. Detailed information about the search mechanisms is provided in the following subparagraphs.

The Candidate List will contain only active RAs that are extractable by the user according to the local group/user assignments. The total number of RAs in the Candidate List will be displayed on the main screen.

4.2.1.1.1 List RA IDs. The user will be able to select domain(s) and enter a wildcard RA ID that will be used to search for RAs. The default domain(s) displayed will be based on the user's search configuration, as detailed in paragraph 4.2.1.6.1. The default wildcard RA ID will be *****. The RAs that make up the Candidate List must: (1) meet the search criteria (domain(s) and wildcard RA ID) entered by the user; (2) be in an active state; and (3) be accessible to the user based on the access rights defined by group assignments.

The user will have the option to Append or Replace the resulting RAs to the current Candidate List. If a Candidate List does not currently exist, then a new Candidate List will be displayed in alphabetical order based on the RA ID for both the Append and Replace options. If the user chooses to append the RAs and a Candidate List currently exists, any duplicate RAs will be eliminated and any new candidate RAs will be appended; the entire list will be sorted in alphabetical order by the RA ID. If the user chooses to replace the RAs and a Candidate List currently exists, then the entire Candidate List will be replaced with the new candidate RAs sorted in alphabetical order based on the RA ID.

4.2.1.1.2 List RA Names. The user will be able to select domain(s), and enter a wildcard RA Name that will be used to search for RAs. The default domain(s) displayed will be based on the user's search configuration, as detailed in paragraph 4.2.1.6.1. The default wildcard RA Name will be *****. The RAs that will make up the Candidate List must: (1) meet the search criteria (domain(s) and wildcard RA Name) entered by the user; (2) be in an active state; and (3) be accessible to the user based on the access rights defined by group assignments.

The user will have the option to Append or Replace the resulting RAs to the current Candidate List. If a Candidate List does not currently exist, then a new Candidate List will be displayed in alphabetical order based on the RA Name for both the Append and Replace options. If the user chooses to append the RAs and a Candidate List currently exists, any duplicate RAs will be eliminated and any new candidate RAs will be appended; the entire list will be sorted in alphabetical order by the RA Name. If the user chooses to replace the RAs and a Candidate List currently exists, then the entire Candidate List will be replaced with the new candidate RAs sorted in alphabetical order based on the RA Name.

4.2.1.1.3 Find Keywords. The user will be able to select domain(s) and enter keywords that will be used to search for RAs. The default domain displayed will be based on the user's search configuration, as detailed in paragraph 4.2.1.6.1. The system will search the repository for RAs in which the keywords can be found in the domain(s) selected by the user. The RAs

that meet the search criteria (domain(s) and keyword(s) located in the abstract files) will make up the Candidate List.

The user will have the option to Append or Replace the resulting RAs to the current Candidate List. If a Candidate List does not currently exist, then a new Candidate List will be displayed in alphabetical order based on the RA Name for both the Append and Replace options. If the user chooses to append the RAs and a Candidate List currently exists, any duplicate RAs will be eliminated and any new candidate RAs will be appended; the entire list will be sorted in alphabetical order by the RA Name. If the user chooses to replace the RAs and a Candidate List currently exists, then the entire Candidate List will be replaced with the new candidate RAs sorted in alphabetical order based on the RA Name.

4.2.1.1.4 Catalog Index (WWW). The user will be able to view the list of RAs in the catalog via the WWW page. When the user chooses this option, the system will launch the WWW browser specified by the user, as stated in paragraph 4.2.1.6.3. The user will then be able to view a list of all available RAs and any detailed information available for the RA via hypertext links. The RA Information accessed is stored and maintained on the WWW. When the user exits the WWW browser, the system will return to the state of the system before the WWW browser was launched. This capability will assist users in locating potential RAs.

4.2.1.2 Browse RA Information. The Browse function will not be accessible to the user until a Candidate List exists and an RA on the list is selected. The user will be able to review the following information about the selected RA from the Candidate List: classification, file list (including the abstract, source, document, and problem report files), related RAs, and metrics.

4.2.1.2.1 Browse RA File List. The user will be able to review the list of files available for an RA. The file list will include the abstract file, source files, document files, and problem report files. The RA ID and RA Name will be displayed with the following information for each file:

a. **Type of File.** Each file will be one of the following types and will be sorted in the following order: "Abstract", "Source", "Document", and "Problem Report".

b. **Title and Version.** The title and version of each file will be displayed. Each type of file in the list will be sorted by the version.

c. **File Size (KB).** The total size, in kilobytes, of the RA file.

d. **File Format.** The file format will be "Text" or "Binary".

4.2.1.2.1.1 View RA Files. The user will be able to review the contents of the following types of RA files: Abstract, Document, and Problem Report. The RA file will be transferred from the server where the file is stored to the user's client environment using TCP/IP Asset Transfer Interface.

If an association exists in the user's client environment between the filename extension (of the RA file transferred) and an application, then the system will launch that application and open the RA file at the same time. For non-associated text files, the user will be able to display the contents of the file in a generic text viewer. The size of the RA files to be viewed will be restricted only by the available memory at runtime and available disk space.

4.2.1.2.2 Browse Metrics. The user will be able to review all existing metric values for an RA. At a minimum, all RAs will have values for the Uses and Problem Reports metrics. The user will also have the option to double-click on a metric in the list to analyze the entire Candidate List based on the metric selected. Refer to paragraph 4.2.1.3 for detailed information on the Analyze function.

4.2.1.2.3 Browse Related RA List. The user will be able to review the list of all active RAs that are identified as related to the primary RA. Each RA ID in the related RA list will be displayed; visibility of each related RA will be indicated according to the related RA's entry, or absence, in any of the local group/RA assignments.

4.2.1.2.4 Browse Catalog Page (WWW). The user will be able to review information stored about an RA via the WWW page. The RA Information accessed is stored and maintained on the WWW. When this option is selected, the WWW browser will be launched and will display the WWW page configured for the RA selected. Once the WWW page is displayed, the user will be able to perform operations available for the WWW browser (e.g., hypertext links). When the user exits the WWW browser, the system will be displayed in the state in which it was before the WWW browser was launched.

4.2.1.3 Tools. The system will provide the capability to analyze the candidate RAs based on available metrics, clear local catalog information, and sort the candidate RAs based on the RA ID or RA Name.

4.2.1.3.1 Analyze RA List. The Analyze function will not be accessible to the user until a Candidate List exists. The Analyze screen will display the selected Candidate RAs (or all RAs on the Candidate List if none are explicitly selected) in a bar graph form representing the metric value for each RA. The actual value of each metric will also be indicated on each bar. The user will be able to change the type of metric and the sort order of the RAs in the Analyze screen. The user will also be able to reorder the Candidate List with the order selected in the Analyze screen.

4.2.1.3.1.1 Metric Used to Analyze. The user will be able to select from a list of available metrics on which the sort will be based. When the user selects another metric, the Analyze screen will be updated to display the candidate RAs with the new metric values. By default, the list will be ordered by the "None" sort type (as the Candidate List is ordered); otherwise, the list will be sorted by the sort type previously selected for the metric.

4.2.1.3.1.2 Sort RA List. For each metric, the user will be able to reorder RAs in the Analyze screen to be in ascending order, descending order, or as ordered in the current Candidate List ("None" sort type option). The Analyze screen will initially be displayed in the same order as the current Candidate list ("None" sort type).

4.2.1.3.1.3 Apply Order to the Candidate List. The user may reorder the Candidate List with the order selected in the Analyze function. The user will be returned to the main screen with the Candidate List reordered.

4.2.1.3.2 Clear Local Catalog. The user will be able to clear the information stored in the local catalog. This option will not be available when a user is connected to the server.

4.2.1.3.3 Sort Candidate List. The user will be able to sort (alphabetically) the list of candidate RAs based on the RA ID or RA Name.

4.2.1.4 Extract RAs. Based on the asset's availability for extraction and the asset's availability to the user, a user will be able to select files for extraction that are associated with active RAs and active related RAs. As part of a user's request for the extraction of asset files, a local site server will be able to contact another site (local, remote, or foreign) containing the RA and retrieve the RA and any of its associated files. A user will be able to extract files associated with a local asset if it is assigned to any group to which the user is assigned. For remote RAs, the RA's catalog information must be in the user's local catalog, and the user's site must also have been granted extractability to a group containing the asset at the remote site. For programmer-level users, a use log entry will be made at the site from which the RA files are extracted. Also, the sytem will log each local, remote, and foreign extract attempt, including the result of the extract attempt and the file transfer statistics. For foreign RAs, the RA's catalog information must be in the user's local catalog and the foreign site must have granted extractability rights to the user's site (using procedures defined and used at the foreign site).

The user may select the extraction method to be used from a menu of available protocols and methods. The following extraction methods will be supported: File Copy, Tape Copy, Hard Copy, and FTP. For the File Copy and FTP extraction methods, status bars will display the completion status of the current file, the current RA, and the entire extract process.

The User Tool for MS-Windows will support the requirement for a Remote FTP Extract from a local site to a remote host. Additional functionality in the DSRS User Tool will support the Remote FTP Extract from a remote site to a remote host on Sun Solaris 2.3 and Sun OS 4.1.3. The user may select the FTP method from a list of available protocols and methods. File Transfer Protocol (FTP) is a TCP/IP utility that is the Internet standard for file transfer. For Remote FTP Extract to work correctly from the local server site, the UNIX FTP utility must reside in, or have a symbolic link to, the */usr/ucb* directory. FTP requires an account to login to the remote destination host.

4.2.1.4.1 File Copy. The user will be able to copy the selected RA files (which may include Source, Abstract, Document, and Problem Report files) to the client directory. The File Copy

option copies the contents of the extraction to the user's local directory. This option will support RA file transfer using the TCP/IP Asset Transfer Interface.

Incremental status bar updates will display the percentage of the extraction completed for the current file, the current RA, and the entire list of RA files.

4.2.1.4.2 Tape Copy. The Tape Copy option will support RA file transfer by sending a request to the Librarian for a tape containing the selected RA files. This request will be sent to the Librarian(s) at the site(s) where the RA files physically reside. The Librarian must send the tape to the user using an external means.

4.2.1.4.3 Hard Copy. The Hard Copy option will support RA file transfer by sending a request for the selected RA files to the Librarian. This request will be sent to the Librarian(s) at the site(s) where the RA files physically reside. The Librarian must send the hard copy to the user using an external means.

4.2.1.4.4 FTP. The Remote FTP Extract option will support local site RA file transfer by redirecting the contents of the extraction to a user-specified remote destination host.

A remote destination host refers to a user-specified destination machine for extracted RA files. NOTE: If you plan to extract files to an MS-Windows remote destination host, file name conventions may cause undesirable filename corruption. The following paragraphs describe the information to be input by the user:

a. **Host Name**. The known Internet hostname or IP address of the destination host. The hostname is required.

b. **User Name**. The login name of the user used for authentication at the remote host. The username is required.

c. **Password**. The password associated with a login name to use for authentication at the remote destination host. The password is required.

d. **Remote Path**. **(Advanced FTP Option)** The directory path on the remote destination host to which you wish the RA file(s) to be transferred. The remote path defaults to the home directory on the remote destination host.

e. **Port**. **(Advanced FTP Option)** Display the default Internet port for FTP (i.e., 21).

f. **Account**. **(Advanced FTP Option)** The supplemental password to use for access to restricted resources at the remote destination host. The account is not

required. Incremental status bar updates will display the percentage of the extraction completed for the current file, the current RA, and the entire list of RA files.

4.2.1.5 Sessions. The current session filename will be displayed in the title bar of the main screen. If the user has created a new session, then the system will update the title bar when the user saves the session.

4.2.1.5.1 New Session. The user will be able to clear the current session (clear the current Candidate List and domains listed on the main screen). When this option is selected and a Candidate List currently exists, the user will be prompted to save any changes that have been made to the session information. If the user chooses to save the session, the system will save the session as detailed in 4.2.1.5.3 and will then clear the main screen. If the user chooses not to save the session, the system will clear the main screen and discard the current Candidate List and domains displayed. The user will also have the option to cancel this operation.

4.2.1.5.2 Retrieve Session. The user will be able to retrieve previously saved session files. When this option is selected and a Candidate List exists, the user will be prompted to save any changes that have been made to the current session. If the user chooses to save the session, the system will save the session as detailed in 4.2.1.5.3 and will then display the Retrieve Session screen. If the user chooses not to save the session, the system will display the Retrieve Session screen and discard the current session information. The user will also have the option to cancel this operation.

From the Retrieve Session screen, the user will be able to select a session file to be restored. The user will also have the option to cancel this operation.

4.2.1.5.3 Save Session. The user will be able to save the current session, including the RAs in the current Candidate List and domains that were used to build the Candidate List. (The current session file will be indicated in the title of the main screen.) If the user currently does not have a session file open, then the system will prompt the user to save the session as detailed in paragraph 4.2.1.5.4.

4.2.1.5.4 Save Session As. The user will be able to save a session file, including the RAs in the current Candidate List and the domains that were used to build the Candidate List. The user will be able to select the directory and filename for the session file. The default extension for the filename will be ".ses." After the session is saved, the system will display the session filename in the title of the main screen.

4.2.1.6 Options. The user will be able to configure specific options that will be used as the default when the user is executing the tool.

4.2.1.6.1 Preferences. The user will be able to set preferences (defaults) for different user functions. The system will allow users to select a domain to be used as the default when searching for RAs. The system will allow users to specify which default text browser to use when a user chooses to view a text file for which an association does not exist. (Refer to paragraph 4.2.1.2.1.1 for details on viewing file via an association.)

4.2.1.6.2 Network. The system will allow users to enter network configuration information to be used when connecting to the DSRS server. The configuration information includes the DSRS server hostname, the type of server, and the TCP port used when connecting to the server. The user will also be able to test the communication between the client and the server.

4.2.1.6.3 WWW. The system will allow users to enter WWW browser configuration information to be used when the user chooses functions that will launch a WWW browser.

4.2.1.7 Help. The system will provide a Help option from any screen within the system. This option will provide the capability to view on-line information to assist users in operating the system.

4.2.1.7.1 Contents. The system will provide users with a list of available topics from which they can select to view additional information. The help topics will cover such information as an overview of the system, an explanation of user functions, and a description of how to execute the user functions.

4.2.1.7.2 Search Help. The system will provide users the capability to search for help on different topics. The user will be able to select from a list of available topics.

4.2.1.7.3 Tutorial. The system will provide users with an on-line tutorial. The tutorial will instruct beginner users how to execute basic DSRS functions.

4.2.1.8 Exit. The user will be able to log out of the tool. When this option is selected, the user will also be able to save the current session during logout. Refer to paragraph 4.2.1.5.3 for details on saving the current session.

4.2.2 Librarian Tool.

4.2.2.1 RAs. The Supervisor/Librarian will be able to maintain the RA catalog. The catalog will be the collection of RAs, RA Classification, RA File List, RA Metrics, and Related RAs. The system will enforce uniqueness of RA IDs and UIDs (Unique IDs) within the local site catalog.

4.2.2.1.1 RA Information. The Supervisor/Librarian will be able to enter a new RA, retrieve an existing RA, save an RA, or delete an RA.

4.2.2.1.1.1 New RA. The Supervisor/Librarian will be able to clear all fields on the RA screen to allow for input of new RA information. When this option is selected and data exist on the current RA screen, the Supervisor/Librarian will be prompted to save any changes made to the RA information. If the Supervisor/Librarian chooses to save the RA, the system will save all the RA information as detailed in 4.2.2.1.1.3 and will clear all the fields on the screen. If the Supervisor/Librarian chooses not to save the RA, the system will clear all the fields on the screen. The Supervisor/Librarian will have the option to cancel this operation.

4.2.2.1.1.2 Retrieve RA. The Supervisor/Librarian will be able to retrieve RAs by the RA ID, RA Name, or the UID. When this option is selected and data exist on the current RA screen, the Superviosr/Librarian will be prompted to save any changes that have been made to the RA information. If the Supervisor/Librarian chooses to save the RA, the system will save all the RA information as detailed in 4.2.2.1.1.3 and will then display the Retrieve RA screen. If the Supervisor/Librarian chooses not to save the RA, the system will display the Retrieve RA screen. The Supervisor/Librarian will have the option to cancel this operation.

From the Retrieve RA screen, the Supervisor/Librarian will be able to generate a list of RAs using a wildcard for the RA ID, RA Name, or UID. The system will identify all RAs that match the pattern (wildcard ID) entered. The default will display a wildcard RA ID using the user's local site ID (***[local site ID]****). The wildcard may be modified and the system will identify all RAs that match the new pattern. The system will be capable of displaying the number of RA IDs allowed based on available memory at run-time in the Retrieve RA screen.

When the Supervisor/Librarian selects an RA to be retrieved, RA information will be displayed on the RA screen. The Supervisor/Librarian will have the option to cancel this operation.

4.2.2.1.1.3 Save RA. The Supervisor/Librarian will be able to save a new RA or modifications to an existing RA. The following information will be required and validated when the save option is selected:

a. **RA ID and Version.** The RA ID and version will be required for local, remote, and foreign RAs.

b. **RA Name**. The RA Name will be required for local, remote, and foreign RAs.

c. **UID.** The UID will provide the RA with an identifier to support interaction with other interoperability repositories and, therefore, will be unique across all

interoperating repositories. The UID will automatically be generated by the system for new local and remote RAs . The UID generated will be based on the RA ID. The UID for foreign RAs must be entered manually.

d. **State.** The state of the RA will be "Certifying", "Active" or "Archived." Remote and foreign RAs will always be Active. The state will be required for local, remote, and foreign RAs.

e. **Date Submitted.** The system will automatically enter the date the RA was added.

f. **Date Updated.** The system will automatically enter the date the RA was last modified. This date will be null when initially adding an RA.

g. **Point-of-Contact.** The POC will be required for local, remote, and foreign RAs. The POC must be an existing user. The Supervisor/Librarian will be able to select from a list of valid User IDs from the RA screen.

h. **Author.** The author flag will indicate whether the POC is the author of the RA. The default will indicate that the POC is not the author of the asset.

i. **Group Assignments.** The groups that are assigned to the RA will be displayed. The Supervisor/Librarian will have the option to update the list of assigned groups as described in 4.2.2.1.1.6.

When this option is selected, the system will verify that all the required RA information listed above exists. If the RA does not currently exist in the database, then the RA information will be stored. If the RA already exists in the database, the Supervisor/Librarian will be prompted to confirm saving updates to the existing RA.

When saving an Active RA, the system will check for the existance of the following information: RA Classification, Group Assignments, and Files. The Supervisor/Librarian will be warned before leaving the RA screen if any of this information does not exist.

When adding remote RAs, the Supervisor/Librarian will receive the required information from a DSRS export file. (Refer to 4.2.2.10 for details on the Export function.) The Supervisor/Librarian will have the capability to import the remote RA information into the local catalog using the Import function. (Refer to 4.2.2.9 for details on the Import function.) When adding foreign RAs, the Supervisor/Librarian will receive the required information from an index file created by and sent from another interoperability repository. The Supervisor/Librarian will be required to manually add the foreign RA information into the local catalog.

4.2.2.1.1.4 <u>Save RA As.</u> The Supervisor/Librarian will be able to save an existing RA as a new or an existing RA. The same information required for Save RA (4.2.2.1.1.3) will be

required for the Save As operation. All processing will be the same as described in the Save RA section, except a valid RA ID will be required. The existing RA will remain in the system unchanged. The new RA will be a duplicate of selected portions of the existing RA. The system will allow the user to select portions of the RA to be copied, including RA Classification, Related RAs, RA Files, and RA Metrics.

4.2.2.1.1.5 Delete RA. The Supervisor will be able to delete an RA from the catalog. The system will validate that the RA currently exists. The system will prompt the user to confirm the deletion. When an RA is deleted, the following information will automatically be removed from the catalog: the RA Metrics, entries for related RAs, RA Classification, RA File List, and Group Assignments.

4.2.2.1.1.6 Assign Group(s) to RA. The Supervisor/Librarian will be able to add or delete non-wildcard groups assigned to an RA. The Supervisor/Librarian will have the capability to build the list of Assigned Groups from a list of existing unassigned groups. From the Assign Groups to RA screen, the Supervisor/Librarian will be able to generate a list of groups using a wildcard for the Group ID. The system will identify all the groups that match the pattern (wildcard ID) and are not already assigned to the RA. The default wildcard (*****) will display all the available Group IDs. The system will update the list of matching Group IDs if the Supervisor/Librarian changes the wildcard ID. The system will be capable of displaying the number of Group IDs allowed based on available memory at run-time in the Assign Groups to RA screen.

4.2.2.1.2 RA Classification.

4.2.2.1.2.1 New RA Classification. The Supervisor/Librarian will be able to clear the RA ID and classification fields on the RA Classification screen to allow for input of the classification for an existing RA. When this option is selected and data exist on the current RA Classification screen, the Supervisor/Librarian will be prompted to save any changes that have been made to the RA Classification. If the Supervisor/Librarian chooses to save the current RA Classification, the system will save the RA Classification as detailed in 4.2.2.1.2.3 and will then clear all editable fields on the screen. If the Supervisor/Librarian chooses not to save the RA Classification, the system will clear all applicable fields on the screen. The Supervisor/Librarian will have the option to cancel this operation.

4.2.2.1.2.2 Retrieve RA Classification. The Supervisor/Librarian will be able to retrieve the RA Classification for an existing RA. When this option is selected and data exist on the current RA Classification screen, then the Supervisor/Librarian will be prompted to save any changes that have been made to the current RA Classification. If the Supervisor/Librarian chooses to save the RA Classification, the system will save all the classification information as detailed in 4.2.2.1.2.3 and will display the Retrieve RA screen. If the Supervisor/Librarian chooses not to save the RA Classification, the system will display the Retrieve RA screen. The Supervisor/ Librarian will have the option to cancel this operation.

From the Retrieve RA screen, the Supervisor/Librarian will be able to generate a list of RAs as described in Retrieve RA (4.2.2.1.1.2). When the Supervisor/Librarian selects an RA to be

retrieved, the classification for the RA will be displayed on the RA Classification screen. The Supervisor/Librarian will have the option to cancel the retrieve operation.

4.2.2.1.2.3 Save RA Classification. The Supervisor/Librarian will have the capability to save modifications to the RA Classification. The RA Classification will consist of a list of multiple descriptors that will be made up of a domain, facet, and facet term. The Supervisor/Librarian will be able to select from a list of available domains, facets, and facet terms. After a domain, facet (which corresponds to the domain), and facet term (which corresponds to the facet) are selected, the system will provide the capability to add the descriptor to the RA Classification.

When this option is selected, the Supervisor/Librarian will be prompted to confirm saving the updates to the existing RA Classification. The size of the RA Classification will be restricted only by the available memory at runtime. The following will be required and validated when the save option is selected:

a. **Domain.** The domain will be selected from the list of available domains.

b. **Facet.** The facet will be selected from the list of available facets corresponding to the domain selected.

c. **Facet Term.** The facet term will be selected from the list of facet terms corresponding to the facet selected.

4.2.2.1.2.4 Save RA Classification As. The Supervisor/Librarian will be able to save an existing RA Classification as a new RA Classification. The same information required for Save RA Classification (4.2.2.1.2.3) will be required for the Save As operation. All processing will be the same as described in the Save RA Classification section, except the system will prompt for an existing RA ID. If an RA Classification entry exists for the specified RA ID, the system will replace the existing entry after user confirmation.

4.2.2.1.2.5 Delete RA Classification. The Supervisor/Librarian will be able to delete a descriptor from the classification of an existing RA in the catalog. The Supervisor/Librarian will also be able to delete the entire classification of an existing RA. The Supervisor/Librarian will be prompted to confirm deletion of the entire RA Classification.

4.2.2.1.3 Related RAs. The Supervisor/Librarian will be able to maintain related RAs for RAs in the catalog. “Related” refers to the association of one RA to another RA in the repository. When a related RA exists for an RA, then the system will establish an association between the RAs.

4.2.2.1.3.1 New Related RAs. The Supervisor/Librarian will be able to clear all the editable fields on the Related RAs screen to allow for modifications to the Related RA list for an existing RA. When this option is selected and data exist on the current Related RA screen, the Supervisor/Librarian will be prompted to save any changes that have been made to the Related RA list. If the Supervisor/Librarian chooses to save the current Related RA List, the system will save the list as detailed in 4.2.2.1.3.3 and will clear all the fields on the screen. If the Supervisor/Librarian chooses not to save the Related RA List, the system will clear all the fields on the screen and discard the current Related RA List. The Supervisor/Librarian will have the option to cancel this operation.

4.2.2.1.3.2 Retrieve Related RAs. The Supervisor/Librarian will be able to retrieve the Related RA list for an existing RA. When this option is selected and data exist on the current Related RAs screen, the Supervisor/Librarian will be prompted to save any changes that have been made to the current Related RA list. If the Supervisor/Librarian chooses to save the list, the system will save the list as detailed in 4.2.2.1.3.3 and will then display the Retrieve RA screen. If the Supervisor/Librarian chooses not to save the list, the system will display the Retrieve RA screen. The Supervisor/Librarian will have the option to cancel this operation.

From the Retrieve RA screen, the Supervisor/Librarian will be able to generate a list of RAs as described in Retrieve RA (4.2.2.1.1.2). When the Supervisor/Librarian selects an RA to be retrieved, the list of Related RAs for the RA will be displayed. The Supervisor/Librarian will have the option to cancel the retrieve operation.

4.2.2.1.3.3 Save Related RAs. The Supervisor/Librarian will be able to save modifications to the Related RA list of an existing RA in the catalog. The total number of related RAs that may be added to the catalog will be restricted only by the available memory at runtime. The following information will be displayed for each RA related to the primary RA:

a. **Relationship.** The type of relationship that will be established between the primary and the related RA. The Supervisor/Librarian will be able to select from a list of available types of relationships.

b. **Related RA ID.** The RA that will become related to the primary RA. The Supervisor/Librarian will be able to select from a list of available RA IDs. The Supervisor/Librarian will be able to generate the list of available RA IDs using a wildcard.

c. **RA Name.** The system will automatically display the RA Name when the Supervisior/Librarian assigns the RA to the Related RA list.

d. **State.** The system will automatically display the state of the Related RA when the Supervisor/ Librarian assigns the RA to the Related RA list.

When this option is selected, the system will automatically generate the inverse relationship between the primary and each related RA. For relationships that are flagged as "generate trace", the system will create the appropriate relationships. The Supervisor/Librarian will be prompted to save the updates to the existing Related RA list.

4.2.2.1.3.4 Save Related RAs As. The Supervisor/Librarian will be able to save an existing Related RA list as the Related RA list for an existing RA. The same information required for Save Related RAs (4.2.2.1.3.3) will be required for the Save As operation. All processing will be the same as described in the Save Related RAs section, except the system will prompt for an existing RA ID. If a Related RA List exists for the specified RA ID, the system will replace the existing entry after user confirmation.

4.2.2.1.3.5 Delete Related RAs. The Supervisor/Librarian will be able to delete an RA from the Related RA list for an existing RA. The Supervisor/Librarian will be prompted to confirm deletion of the Related RA list.

4.2.2.1.4 RA Metrics. The Supervisor/Librarian will be able to retrieve, clear, and save the metric values for an RA, except for the Problem Reports and Uses metrics. Each RA has a subset of the total set of metrics. This subset must include non-null values for the Problem Reports metric and the Uses metric. The system will generate and maintain the Problem Reports and Uses metrics. The list will contain only non-null numeric metric values and will be capable of representing seven positions.

4.2.2.1.4.1 New RA Metrics. The Supervisor/Librarian will be able to clear all the fields on the RA Metrics screen to allow for input of metrics for an existing RA. When this option is selected and data exist on the current RA Metrics screen, the Supervisor/Librarian will be prompted to save any changes that have been made to the RA Metrics. If the Supervisor/Librarian chooses to save the current RA Metrics, then the system will save all the metrics as detailed in section 4.2.2.1.4.3 and will then clear all the fields on the screen. If the Supervisor/Librarian chooses not to save the RA Metrics, the system will clear all the fields on the screen. The Supervisor/Librarian will have the option to cancel this operation.

4.2.2.1.4.2 Retrieve RA Metrics. The Supervisor/Librarian will be able to retrieve the RA Metrics for an existing RA. The system will display a zero value for all existing metric types that are not present in the RA Metrics list for the selected RA. When this option is selected and data exist on the current RA Metrics screen, then the Supervisor/Librarian will be prompted to save any changes that have been made to the current RA Metrics. If the Supervisor/Librarian chooses to save the RA Metrics, then the system will save all the metrics as detailed in 4.2.2.1.4.3 and will then display the Retrieve RA screen. If the Supervisor/Librarian chooses not to save the RA Metrics, then the system will display the Retrieve RA screen. The Supervisor/Librarian will have the option to cancel this operation.

From the Retrieve RA screen, the Supervisor/Librarian will be able to generate a list of RAs as described in Retrieve RA (4.2.2.1.1.2). When the Supervisor/Librarian selects an RA to be retrieved, the metrics for the RA will be displayed on the RA Metrics screen. The Supervisor/Librarian will have the option to cancel the retrieve operation.

4.2.2.1.4.3 Save RA Metrics. The Supervisor/Librarian will be able to save modifications to the metrics for an existing RA in the catalog. The Supervisor/Librarian will be able to enter values for each available metric type (except for the Uses and Problem Report metric types) displayed on the RA Metric screen. The system generates and maintains the Uses and Problem Report metric types. Any metrics, other than the Uses and Problem Report metrics, with values equal to zero will not be stored in the system.

When this option is selected, the system Supervisor/Librarian will be prompted to save the updates to the existing RA Metrics.

4.2.2.1.4.4 Save RA Metrics As. The Supervisor/Librarian will be able to save existing metric values as the metric values for an existing RA. The same information required for Save RA Metrics (4.2.2.1.4.3) will be required for the Save As operation. All processing will be the same as described in the Save RA Metrics section, except the system will prompt for an existing RA ID. If metric values exist for the specified RA ID, the system will replace the existing entry after user confirmation. All metrics will be copied, except for the Uses and Problem Report metrics. The Uses metric will be set to zero and all use log entries will be deleted for the destination RA. The Problem Report metric will be updated to reflect the number of problem report RA files associated with the destination RA.

4.2.2.1.5 RA Files. The Supervisor/Librarian will be able to maintain the file list for RAs in the catalog.

4.2.2.1.5.1 New RA File List. The Supervisor/Librarian will be able to clear all the fields on the RA Files screen to allow for input of RA files for an existing RA. When this option is selected and data exist on the current RA Files screen, the Supervisor/Librarian will be prompted to save any changes that have been made to the RA File list. If the Supervisor/Librarian chooses to save the current RA File list, the system will save the list as detailed in 4.2.2.1.5.3 and will clear all the fields on the screen. If the Supervisor/Librarian chooses not to save the list, the system will clear all the fields on the screen. The Supervisor/Librarian will have the option to cancel this operation.

4.2.2.1.5.2 Retrieve RA File List. The Supervisor/Librarian will be able to retrieve the RA File list for an existing RA. When this option is selected and data exist on the current RA Files screen, the Supervisor/Librarian will be prompted to save any changes that have been made to the current RA File list. If the Supervisor/Librarian chooses to save the list, the system will save the list as detailed in 4.2.2.1.5.3 and will display the Retrieve RA screen. If the Supervisor/Librarian chooses not to save the list, the system will display the Retrieve RA screen. The Supervisor/Librarian will have the option to cancel this operation.

From the Retrieve RA screen, the Supervisor/Librarian will be able to generate a list of RAs as described in Retrieve RA (4.2.2.1.1.2). When the Supervisor/Librarian selects an RA to be retrieved, the list of RA files for the RA will be displayed on the RA Files screen. The Supervisor/Librarian will have the option to cancel the retrieve operation.

4.2.2.1.5.3 Save RA File. The Supervisor/Librarian will be able to save the list of files for an existing RA. The total number of files that may exist in the system will be restricted only by the available memory at runtime. The following information will be required for each RA file in the list:

a. **Title.** The title of the file that will be saved.

b. **Version.** The version of the file that will be saved.

c. **Type.** The file type will be "Abstract", "Source", "Document", or "Problem Report".

d. **Filename.** The filename will be required and validated for local RAs. For remote RAs, the system will automatically enter "Remote RA" for the filename. For foreign RAs, the system will automatically enter "Foreign RA" for the filename.

e. **File Format.** The file format will be "Text" (default) or "Binary".

f. **File Size.** The size of the RA file in kilobytes (KB) will be initialized to 0.

g. **RA Size.** The total size, in kilobytes, of all the RA files associated with the RA. The system will automatically calculate the RA size.

When this option is selected, the Supervisor/Librarian will be prompted to save the updates to the existing RA File list.

4.2.2.1.5.4 Save RA Files As. The Supervisor/Librarian will be able to save an existing RA File list as the RA File list for an existing RA. The same information required for Save RA Files (4.2.2.1.5.3) will be required for the Save As operation. All processing will be the same as described in the Save RA Files section, except the system will prompt for an existing RA ID. If an RA File list exists for the specified RA ID, the system will replace the existing entry after user confirmation.

4.2.2.1.5.5 Delete RA File. The Supervisor/Librarian will be able to delete an RA File list. The Supervisor/Librarian will be prompted to confirm deletion of the RA File list.

4.2.2.2 Groups. The Supervisor/Librarian will be able to maintain groups and group assignments.

4.2.2.2.1 New Group. The Supervisor/Librarian will be able to clear all the fields on the Group screen to allow for input of new group information. When this option is selected and data exist on the current Group screen, the Supervisor/Librarian will be prompted to save any changes that have been made to the group information. If the Supervisor/Librarian chooses to save the group, then the system will save all group information as detailed in 4.2.2.2.3 and will clear all fields on the screen. If the Supervisor/Librarian chooses not to save the group, the system will clear all fields on the screen. The Supervisor/Librarian will have the option to cancel this operation.

4.2.2.2.2 Retrieve Group. The Supervisor/Librarian will be able to retrieve groups by the Group ID. When this option is selected and data exist on the current group screen, the Supervisor/Librarian will be prompted to save any changes that have been made to the group information. If the Supervisor/Librarian chooses to save the group, the system will save all of the group information as detailed in 4.2.2.2.3 and will display the Retrieve Group screen. If the Supervisor/Librarian chooses not to save the group, the system will display the Retrieve Group screen. The Supervisor/Librarian will have the option to cancel this operation.

From the Retrieve Group screen, the Supervisor/Librarian will be able to generate a list of groups using a wildcard for the Group ID. The system will identify all the groups that match the pattern (wildcard Group ID) entered. The default will display a wildcard Group ID (*). The wildcard may be modified and the system will identify all the groups that match the new pattern. The system will be capable of displaying the number of Group IDs allowed based on available memory at runtime on the Retrieve Group screen.

When the Supervisor/Librarian selects a group to be retrieved, the group information will be displayed on the Group screen. The Supervisor/Librarian will have the option to cancel this operation.

4.2.2.2.3 Save Group. The Supervisor/Librarian will be able to save a new group or modifications to an existing group. The total number of groups that may be added to the system will be restricted only by the available memory at runtime. The following paragraphs indicate the information that may be required and validated when the save option is selected:

a. **Group ID.** The unique name for the group. The Group ID will be required and will be verified for uniqueness.

b. **Description.** The description of the group. The description will not be required.

c. **RA Assignments.** The RAs currently assigned to the group will be displayed. The Supervisor/Librarian will have the option to update the list of RAs assigned to the group.

d. **Site Assignments.** The sites currently assigned to the group will be displayed. The Supervisor/Librarian will have the option to update the list of sites assigned to the group.

e. **User Assignments.** The users currently assigned to the group will be displayed. The Supervisor/Librarian will have the option to update the list of users assigned to the group.

When this option is selected, the system will verify that all the required group information listed above exists. If the group does not currently exist in the database, the group information will be stored. If the group already exists in the database, the Supervisor/Librarian will be prompted to save the updates to the existing group.

4.2.2.2.4 Save Group As. The Supervisor/Librarian will be able to save an existing group as a new group. The same information required for Save Group (4.2.2.2.3) will be required for the Save As operation. All processing will be the same as described in the Save Group section, except a valid Group ID will be required. All RA assignments, site assignments, and user assignments will be duplicated in the new group. If the specified Group ID exists, the system will replace the existing entry after user confirmation.

4.2.2.2.5 Delete Group. The Supervisor/Librarian will be able to delete a group. The system will validate that the Group ID currently exists. The system will prompt the Supervisor/Librarian to confirm the deletion. When a group is deleted, all the group assignments that exist for the group will also be deleted from the database.

4.2.2.2.6 Group Assignments. The Supervisor/Librarian will be able to assign RAs, users, and sites to groups. When creating group assignments, the Group ID will be required. These group assignments will allow the Supervisor/Librarian to manage and control users' access to assets. A group assignment will identify a collection of RAs, users, and sites, and will convey certain rights and privileges to the members of that collection. A user's membership in a group will grant extraction permission to the assets that are also members of the group.

4.2.2.2.6.1 Assign RA(s) to Group. The Supervisor/Librarian will be able to add or delete RAs to group assignments. From the Assign RAs to Group screen, the Supervisor/Librarian will be able to generate a list of RAs using a wildcard for the RA ID. The system will identify all the RAs that match the pattern (wildcard ID) and are not already assigned to the group. The default will display a wildcard RA ID using the local site ID (***[local site ID]****). The system will update the list of matching RA IDs if the Supervisor/Librarian changes the wildcard ID. The system will be capable of displaying the number of RA IDs allowed based on available memory at run-time on the Assign RAs to Group screen.

The Supervisor/Librarian will have the capability to transfer any available RA IDs to the currently assigned RA IDs displayed, and vice versa. The Supervisor/Librarian may transfer individual RA IDs, multiple RA IDs, or a token indicating all the RAs belonging to a site in the repository. When the token exists in the list of assigned RA IDs, all the RAs in the repository will be assigned to the group, as will any new RAs that are added to the repository.

4.2.2.2.6.2 Assign User(s) to Group. The Supervisor/Librarian will be able to add or delete users to a group assignment. From the Assign Users to Group screen, the Supervisor/Librarian will be able to generate a list of users using a wildcard for the User ID. The system will identify all the users that match the pattern (wildcard ID) and are not already assigned to the group. The default will display a wildcard User ID (*). The system will update the list of matching User IDs if the Supervisor/Librarian changes the wildcard ID. The system will be capable of displaying the number of User IDs allowed based on the available memory at run-time in the Assign Users to Group screen.

The Supervisor/Librarian will have the capability to transfer any of the available User IDs to the currently assigned User IDs displayed, and vice versa. The Supervisor/Librarian may transfer individual User IDs, multiple User IDs, or a token indicating all the users in the repository. When the token exists in the list of assigned User IDs, all the users in the repository will be assigned to the group, as will any new Users that are added to the repository.

4.2.2.2.6.3 Assign Site(s) to Group. The Supervisor/Librarian will be able to add or delete sites to group assignments. From the Assign Sites to Group screen, the Supervisor/Librarian will be able to generate a list of sites using a wildcard for the Site ID. The system will

identify all the sites that match the pattern (wildcard ID) and are not already assigned to the group. The default wildcard (*****) will display all the available Site IDs. The system will update the list of matching Site IDs if the Supervisor/Librarian changes the wildcard ID. The system will be capable of displaying the number of Site IDs allowed based on the available memory at run-time in the Assign Sites to Group screen.

The Supervisor/Librarian will have the capability to transfer any of the available Site IDs to the currently assigned Site IDs displayed and vice versa. The Supervisor/Librarian may transfer individual Site IDs, multiple Site IDs, or a token indicating all the sites in the repository. When the token exists in the list of assigned Site IDs, then all the sites in the repository will be assigned to the group, as will any new sites that are added to the repository.

4.2.2.3 Users. The Supervisor/Librarian will be able to maintain users and user assignments. **Only Supervisors will be able to perform operations on supervisor-level users.**

4.2.2.3.1 New User. The Supervisor/Librarian will be able to clear all the fields on the User screen to allow for input of new user information. When this option is selected and data exist on the current User screen, then the Supervisor/Librarian will be prompted to save any changes that have been made to the user information. If the Supervisor/Librarian chooses to save, the system will save all the user information as detailed in 4.2.2.3.3 and will clear all the fields on the screen. If the Supervisor/Librarian chooses not to save, the system will clear all the fields on the screen. The Supervisor/Librarian will have the option to cancel this operation.

4.2.2.3.2 Retrieve User. The Supervisor/Librarian will be able to retrieve users by the User ID. When this option is selected and data exist on the current User screen, the Supervisor/Librarian will be prompted to save any changes that have been made to the user information. If the Supervisor/Librarian chooses to save, then the system will save all the user information as detailed in Save User (4.2.2.3.3) and will display the Retrieve User screen. If the Supervisor/Librarian chooses not to save, the system will display the Retrieve User screen. The Supervisor/Librarian will have the option to cancel this operation.

From the Retrieve User screen, the Supervisor/Librarian will be able to generate a list of users using a wildcard for the User ID. The system will identify all of the users that match the pattern (wildcard ID) entered. The default will display a wildcard User ID (*****). The wildcard may be modified and the system will identify all the User IDs that match the new pattern. The system will be capable of displaying the number of User IDs allowed based on the available memory at run-time in the Retrieve User screen.

When the Supervisor/Librarian selects a user to be retrieved, the user information will be displayed on the User screen. The Supervisor/Librarian will have the option to cancel this operation.

4.2.2.3.3 Save User. The Supervisor/Librarian will be able to save a new user or modification to an existing user. The total number of users that may be added to the system will be restricted only by the available memory at runtime. The following information will be required (unless otherwise specified) and validated to save a user:

a. **User ID.** The user identifier will be required and verified for uniqueness.

b. **User Name.** The name of the user that will be added to the system will be required.

c. **Password.** The password for the user will be required (except for non-user type users).

d. **Type of User.** The type of system user will be required and must be one of the following types:

(1) **Non-User.** A person who is identified in the system as being a point-of-contact (POC) for an RA. A non-user will not be able to gain access to the system.

(2) **Programmer.** A person who will be able to execute the User Tool to identify RAs.

(3) **Librarian.** A person who maintains the repository. This type of user will be able to execute all the functions except for the following: delete an RA; delete a domain; delete a facet; maintain local, remote, or foreign site information; and maintain supervisor-level user information.

(4) **Supervisor.** A person who maintains the repository. This type of user will be able to execute all of the functions associated with the system.

e. **Phone.** The user's telephone number will be required.

f. **E-mail Address.** The user's e-mail address will not be required.

g. **Organization.** The user's organization will not be required.

h. **Address.** The address will include the following items: mail stop, street, city, state, Zip code, and country. The user's address will not be required.

i. **Password Duration.** The duration in days after the user's Password is changed before the user will be required to change the password again.

j. **Expiration Date.** The day on which the user's password will expire will not be required.

k. **Locked.** Indicates that the account has been disabled due to login failures.

l. **Number of Logins.** Indicates the number of times the user has successfully logged into the system. This value is generated by the system.

m. **Last Login Date.** The date when the user last logged into the system. This value is generated by the system.

n. **Memo/Comments.** Allows comments or notes on the user account to be entered. This field will not be required.

When this option is selected, the system will verify that all the required user information listed above exists. If the user does not currently exist in the database, the user information will be stored. If the user already exists in the database, then the Supervisor/Librarian will be prompted to save the updates to the existing user.

4.2.2.3.4 Save User As. The Supervisor/Librarian will be able to save an existing User as a new or existing user. The same information required for Save User (4.2.2.3.3) will be required for the Save As operation. All processing will be the same as described in the Save User section, except a valid User ID and password will be required. This functionality will provide the Supervisor/Librarian with the capability to copy user information from existing users.

4.2.2.3.5 Delete User. The Supervisor/Librarian will be able to delete a user. The system will validate that the User ID currently exists. The system will prompt the Supervisor/Librarian to confirm the deletion. When the Supervisor/Librarian selects to delete a user, all the user information and group to user assignments will be deleted from the repository. The system will not allow the last Supervisor user to be deleted from the system.

4.2.2.3.6 Assign Group(s) to User. The Supervisor/Librarian will be able to add or delete non-wildcard group to user assignments. From the Assign Groups to User screen, the Supervisor/Librarian will be able to generate a list of groups using a wildcard for the Group

ID. The system will identify all the groups that match the pattern (wildcard ID) and are not already assigned to the user. The default wildcard (*****) will display all the available Group IDs. The system will update the list of matching Group IDs if the Supervisor/Librarian changes the wildcard ID. The system will be capable of displaying the number of Group IDs allowed based on the available memory at run-time in the Assign Groups to User screen.

The Supervisor/Librarian will have the capability to transfer any of the available Group IDs to the currently assigned Group ID list and vice versa. The Supervisor/Librarian may transfer individual Group IDs and multiple Groups IDs.

4.2.2.4 Sites. The Supervisor will be able to maintain the local, remote, and foreign site information. The Librarian will be able to retrieve to view local, remote, and foreign site information. The system will enforce uniqueness of the site IDs within the local site catalog. The site information will be used in forming and validating RA IDs and other repository information and to control access from remote and foreign sites. The total number of remote sites that may be added to the system will be restricted only by the available memory at runtime and the total number of unique sites possible.

4.2.2.4.1 New Site. The Supervisor/Librarian will be able to clear all the fields on the Site screen to allow for input of new site information. When this option is selected and data exist on the current Site screen, the Supervisor will be prompted to save any changes that have been made to the site information. **The Librarian will not have the privilege to save changes**. If the Supervisor chooses to save the site, the system will save all the site information as detailed in 4.2.2.4.3 and will clear all the fields on the screen. If the Supervisor chooses not to save the site, the system will clear all the fields on the screen. The Supervisor will have the option to cancel this operation.

4.2.2.4.2 Retrieve Site. The Supervisor/Librarian will be able to retrieve sites by the Site ID. When this option is selected and data exist on the current Site screen, the Supervisor will be prompted to save any changes that have been made to the site information. **The Librarian will not have the privilege to save changes**. If the Supervisor chooses to save, the system will save all the site information as detailed in Section 4.2.2.4.3 and will display the Retrieve Site screen. If the Supervisor chooses not to save, the system will display the Retrieve Site screen. The Supervisor will have the option to cancel this operation.

From the Retrieve Site screen, the Supervisor/Librarian will be able to generate a list of sites and site names using a wildcard for the Site ID. The system will identify all the sites that match the pattern (wildcard ID) entered. The default wildcard will display all the existing sites (*). The wildcard may be modified and the system will identify all the site IDs that match the new pattern. The system will be capable of displaying the number of Site IDs allowed based on the available memory at run-time in the Retrieve Site screen.

When the Supervisor/Librarian selects a site to be retrieved, the site information will be displayed on the Site screen. The Supervisor/Librarian will have the option to cancel this operation.

4.2.2.4.3 Save Site. The Supervisor will be able to save a new local, remote, or foreign site or modifications to an existing local, remote, or foreign site. The total number of sites that can be added to the system will be restricted only by available memory at runtime. The following site information will be required to save the site:

a. **Site ID.** The Site ID will be required and will be verified for uniqueness.

b. **Site Name.** The name of the site that will be added to the system will be required.

c. **Library Type.** The type of library (local, remote, or foreign) that exists at the site will be required. The Library Type for the local site will not be editable; only one local site can exist in the database. A remote library is a remote DSRS site that will be interoperable with the local site. A foreign library is a non-DSRS site that will be interoperable with the local site.

d. **Site Supervisor.** The name of the site supervisor will be required.

e. **Phone.** The phone number of the site supervisor will be required.

f. **Hostname.** The hostname of the site will be required.

g. **IP Address.** The Internet Protocol (IP) address of the host will be required.

The following items will be configurable for the local site only:

a. **Login Threshold.** The number of login failures allowed for each user registered at the local site.

b. **Inactivity Timeout.** The duration in seconds of inactivity allowed before a user is automatically logged out of the system.

When this option is selected, the system will verify that all the required site information listed above exists. If the site does not currently exist in the database, the site information will be stored. If the Supervisor has previously retrieved the local site or a foreign site and has changed the associated Site ID, the system will update all RA IDs for the site. If the site

already exists in the database, the Supervisor will be prompted to save the updates to the existing site.

4.2.2.4.4 Save Site As. The Supervisor will be able to save an existing remote site as a new or existing site. The same information required for Save Site (4.2.2.4.3) will be required for the Save As operation, except for the local site options. All processing will be the same as described in the Save Site section, except a valid Site ID will be required. If the new site specified exists, the system will replace the existing entry after user confirmation. This functionality will provide the Supervisor with the capability to copy remote site information from existing remote sites.

4.2.2.4.5 Delete Site. The Supervisor will be able to delete a remote or foreign site from the repository. The system will validate that the Site ID currently exists. The system will prompt the Supervisor to confirm the deletion. When a site is deleted, the following information will also be deleted from the database: site assignments, all RAs and RA information associated with the Site ID, and the group assignments associated with the Site ID.

4.2.2.4.6 Assign Group(s) to Site. The Supervisor/Librarian will be able to add or delete non-wildcard group to site assignments. From the Assign Groups to Site screen, the Supervisor/Librarian will be able to generate a list of groups using a wildcard for the Group ID. The system will identify all the groups that match the pattern (wildcard ID) and are not already assigned to the site. The default wildcard (*****) will display all the available Group IDs. The system will update the list of matching Group IDs if the Supervisor/Librarian changes the wildcard ID. The system will be capable of displaying the number of Group IDs allowed based on the available memory at run-time in the Assign Groups to Site screen.

4.2.2.5 Classification Scheme. The Supervisor will be able to maintain domains, facets, and facet terms that comprise the classification scheme. The Librarian has limited capability for maintaining the classification scheme.

4.2.2.5.1 Domains. The Supervisor will be able to maintain domains in the system. Domains will be used when users formulate the criteria to search for RAs. The options for maintaining domains will include new, retrieve, save, and delete.

4.2.2.5.1.1 New Domain. The Supervisor will be able to add domain information to the catalog. The total number of domains that may be added will be restricted only by the available memory at runtime. The system will enforce uniqueness of the domain names within the local catalog. When this option is selected, the system will display the New Domain screen for input of new domain information.

The following information will be required for each new domain:

a. **Domain Name.** The unique domain name will be required and validated for uniqueness.

b. **Description.** The description for the domain will be required.

If the domain name or description is modified, the system will verify that the domain name is unique and will prompt the Supervisor for confirmation of the changes to the local catalog. If the Supervisor chooses to save, the system will save any changes made to the domain name or description to the local catalog. If the Supervisor chooses not to save, any modifications to the domain name or description will be discarded.

When the Supervisor chooses to save the new domain, the system will verify that all the information listed above exists and will create new Domain Classification tables (for Active RAs) and a new Domain to RA cross-reference table. If the Supervisor chooses not to save, the system will return to the Classification screen without any changes made to the local catalog.

4.2.2.5.1.2 Retrieve Domain. The Supervisor/Librarian will be able to retrieve a domain from a list of available domains in the local catalog. When the Supervisor/Librarian selects a domain to be retrieved, the domain name, domain description, and assigned facets will be displayed on the Classification screen.

4.2.2.5.1.3 Save Domain. The Supervisor will be able to save modifications to the domain name and description from the Classification screen. (Refer to paragraph 4.2.2.5.1.1 for details regarding saving new domain information to the local catalog.)

4.2.2.5.1.4 Save Domain As. The Supervisor will be able to save an existing Domain as a new Domain. The same information required for Save Domain (4.2.2.5.1.3) will be required for the Save As operation. All processing will be the same as described in the Save Domain section, except a new domain name will be required. The system will allow the user to select a portion of the domain to be copied, including the facets assigned to the domain, the facet terms assigned to facets in the domain (if facets are selected to be copied).

4.2.2.5.1.5 Delete Domain. The Supervisor will be able to delete a domain. The system will prompt the Supervisor to confirm the deletion. When a domain is deleted, the following tables and information for the domain will also be deleted: the domain information (domain name, and description), the RA Classification lists, and any facets, and facet terms that exist within the domain.

4.2.2.5.1.6 Assign Facet(s) to Domain. The Supervisor will be able to add or delete facets associated with the selected domain. The Librarian will be able to add facets associated with

the selected domain. The system will provide the Supervisor/Librarian with a list of available facets (in the local catalog) that are not currently assigned to the domain and a list of the currently assigned facets. The Supervisor will have the capability to transfer any of the available facets to the currently assigned facet list and vice versa. The Librarian will be able to transfer facets from the available facet list to the assigned list (adding facets to the assigned list). The Supervisor/Librarian may transfer individual facets, multiple facets, or all the facets in the catalog.

4.2.2.5.2 Facets. The Supervisor/Librarian will be able to maintain facets in the system for the domain selected on the Classification screen. The options for maintaining facets will include new, retrieve, save, and delete.

4.2.2.5.2.1 New Facet. The Supervisor/Librarian will be able to add a new facet and rank to the catalog. The total number of facets that may be added will be restricted only by the available memory at runtime. The system will enforce uniqueness of the facets within each domain in the local catalog. The Supervisor/Librarian will be able to add new facets to a domain by assigning facets that currently exist in the catalog via the Assign Facets to Domain screen (as detailed in paragraph 4.2.2.5.1.6). The Supervisor/Librarian will also be able to add new facets for the selected domain via the New Facet screen. The following information will be added to the local catalog for each new facet:

a. **Domain Name.** The domain name will be required and verified for uniqueness.

b. **Facet Name.** The facet name will be the facet assigned to the domain and will be required.

c. **Rank.** The rank of the facet in relation to the other facets that exist for the domain. The rank will be required.

When the Supervisor/Librarian chooses to save the new facet, the system will verify that all the above information exists and will save the facet information to the local catalog for the selected domain. If the Supervisor/Librarian chooses not to save the information, the system will return to the Classification screen without any modifications to the local catalog. The facet rank of all facets on the system will be reordered to insert the new facet.

4.2.2.5.2.2 Retrieve Facet. The Supervisor/Librarian will be able to select a facet from the list of available facets that currently exists for the selected domain. When the Supervisor/Librarian selects a facet, the system will retrieve and display facet rank and assigned facet terms (for the selected facet) on the Classification screen.

4.2.2.5.2.3 Save Facet. The Supervisor/Librarian will be able to save modifications to the facet and rank that exist for the domain selected. (Refer to paragraph 4.2.2.5.2.1 for details on saving a new facet and rank to the local catalog for the domain selected.) If the facet name or facet rank is modified, then the system will verify that the facet is unique within the domain selected and will prompt the Supervisor/Librarian to confirm the modifications. If the Supervisor/Librarian chooses to save, the system will save any changes made to the facet name and rank. If the Supervisor/Librarian chooses not to save, the system will discard any changes made to the facet name and facet rank.

4.2.2.5.2.4 Delete Facet. The Supervisor will be able to delete a facet. The system will prompt the Supervisor to confirm the deletion. The following information is deleted from the local catalog: the facet information (facet name and rank) associated with the domain selected, all the facet terms associated with the facet, and all the RA Classification descriptors that contain the facet to be deleted.

4.2.2.5.2.5 Assign Facet Term(s) to Facet. The Supervisor/Librarian will be able to add and delete facet terms associated with a facet. The system will provide the Supervisor/Librarian with a list of available facet terms (in the local catalog) that are not currently assigned to the facet and a list of currently assigned facet terms. The Supervisor/Librarian will have the capability to transfer any of the available facet terms to the assigned facet term list and vice versa. Individual facet terms can be transferred.

4.2.2.5.3 Facet Terms. The Supervisor/Librarian will be able to maintain facet terms in the system for the facet and domain selected. The options for maintaining facet terms will include new, retrieve, save, and delete.

4.2.2.5.3.1 New Facet Terms. The Supervisor/Librarian will be able to add new facet term information to the catalog. The total number of facet terms that may be added will be restricted only by the available memory at runtime. The system will enforce uniqueness of the facet terms associated with a facet within each domain in the local catalog. The Supervisor/Librarian will be able to add new facet terms for a facet via the New Facet Term screen. The following information will be added to the local catalog for each facet term:

a. **Domain Name.** The domain name will be required and verified for uniqueness.

b. **Facet Name.** The facet name will be the facet selected and will be required.

c. **Facet Term.** The new facet term that will be added to the system for the facet and domain selected. The facet term will be required and verified for uniqueness.

d. **Facet Term Definition.** The definition will contain the meaning of the new facet term and will be required.

When the Supervisor/Librarian chooses to save the new facet term, the system will verify that all the required information listed above exists and will save the facet information to the local catalog for the selected facet and domain. If the Supervisor/Librarian chooses not to save the information, the system will return to the Classification screen without any changes made to the local catalog.

4.2.2.5.3.2 Retrieve Facet Term. The Supervisor/Librarian will be able to select a facet term from a list of available facet terms in the local catalog associated with the facet and domain selected. When the Supervisor/Librarian selects a facet term to be retrieved, the system will display the facet term definition for that facet term.

4.2.2.5.3.3 Save Facet Term. The Supervisor/Librarian will be able to save facet term information to the system for the facet and domain selected. The total number of facet terms that may be added to the system will be restricted only by the available memory at runtime. (Refer to paragraph 4.2.2.5.3.1 for details on saving a new facet term and definition to the local catalog.) If the facet term or facet term definition is modified, the system will verify that the facet term is unique for the facet and domain selected. The system will prompt the Supervisor/Librarian to save the modifications. If the Supervisor/Librarian chooses to save, the system will save any changes to the local catalog. If the Supervisor/Librarian chooses not to save, the system will discard any of the changes.

4.2.2.5.3.4 Delete Facet Term. The Supervisor/Librarian will be able to delete a facet term associated with the facet and domain selected. The system will prompt the Supervisor/Librarian to confirm the deletion. The following information will be deleted from the local catalog: the selected facet term information (term and definition) associated with the facet and domain selected and all the RA Classification descriptors that contain the facet term associated with the facet and domain selected for deletion.

4.2.2.6 Metrics. The Supervisor/Librarian will be able to maintain metrics. The options for maintaining metrics will include new, retrieve, save, and delete.

4.2.2.6.1 New Metric Type. The Supervisor/Librarian will be able to clear all the fields on the Metric screen to allow for the input of a new type of metric. When this option is selected and data exist on the current Metric screen, the Supervisor/Librarian will be prompted to save any changes that have been made to the metric type. If the Supervisor/Librarian chooses to save, the system will save the metric as detailed in 4.2.2.6.3 and will clear all the fields on the

screen. If the Supervisor/Librarian chooses not to save, the system will clear all the fields on the screen. The Supervisor/Librarian will have the option to cancel this operation.

4.2.2.6.2 Retrieve Metric Type. The Supervisor/Librarian will be able to retrieve the existing types of metrics. When this option is selected and data exist on the current Metric screen, the Supervisor/Librarian will be prompted to save any changes that have been made to the type of metric. If the Supervisor/Librarian chooses to save, the system will save all the data as detailed in 4.2.2.6.3 and will display the Retrieve Metric screen. If the Supervisor/Librarian chooses not to save, the system will display the Retrieve Metric screen. The Supervisor/Librarian will have the option to cancel this operation.

From the Retrieve Metric screen, the Supervisor/Librarian will be able to generate a list of available metrics. The system will identify all the metric types that match the wildcard entered. The default will display a wildcard that will display all the existing metrics. The wildcard may be modified and the system will identify all metric types that match the new pattern. The system will be capable of displaying the number of metric types allowable based on the available memory at run-time on the Retrieve Metric screen.

When the Supervisor/Librarian selects a type of metric to be retrieved, the type of metric will be displayed on the Metric screen. The Supervisor/Librarian will have the option to cancel this operation.

4.2.2.6.3 Save Metric Type. The Supervisor/Librarian will be able to save metrics types. The system will enforce uniqueness of the metric types within the local site catalog. The system will update the RA Metrics list, which includes the updated metric types. The total number of metric types that may be added to the system will be restricted only by available memory at runtime.

4.2.2.6.4 Delete Metric Type. The Supervisor/Librarian will be able to delete metric types from the system. The system will delete all the RA Metric list entries that include the deleted metric types. The system will automatically generate and maintain the Uses and the Problem Reports metrics; therefore, the system will not allow deletion of these metric types.

4.2.2.7 Relationships. The Supervisor/Librarian will be able to maintain RA relationships. The options for maintaining RA relationships will include new, retrieve, save, and delete. Relationships may exist between local and non-local assets.

4.2.2.7.1 New Relationship. The Supervisor/Librarian will be able to clear all the fields on the Relationship screen to allow for input of a new relationship. When this option is selected and data exist on the current Relationship screen, the Supervisor/Librarian will be prompted to save any changes that have been made to the relationship information. If the Supervisor/Librarian chooses to save, the system will save all the relationship information as

detailed in 4.2.2.7.3 and will then clear all the fields on the screen. If the Supervisor/Librarian chooses not to save, the system will clear all the fields on the screen. The Supervisor/Librarian will have the option to cancel this operation.

The following paragraphs indicate the information required to add a new relationship:

a. **RA Relationship.** The type of relationship that will exist between RAs will be required.

b. **Relationship Inverse.** The inverse of a relationship will be required.

c. **Generate Trace.** This flag, "Y" or "N", will be used when establishing relationships between RAs and will be required. When the generate trace flag is set to "Y", the system will automatically generate cascading relationships based upon the RA Relationships.

4.2.2.7.2 Retrieve Relationship. The Supervisor/Librarian will be able to retrieve existing relationships. When this option is selected and data exist on the current Relationship screen, the Supervisor/Librarian will be prompted to save any changes that have been made to the relationship information. If the Supervisor/Librarian chooses to save, the system will save all the relationship information as detailed in 4.2.2.7.3 and will display the Retrieve Relationship screen. If the Supervisor/Librarian chooses not to save, the system will display the Retrieve Relationship screen. The Supervisor/Librarian will also have the option to cancel this operation.

From the Retrieve Relationship screen, the Supervisor/Librarian will be able to generate a list of relationships using a wildcard. The system will identify all the relationships that match the pattern (wildcard) entered. The default wildcard will be to display all the existing relationships (*). The wildcard may be modified and the system will identify all the relationships that match the new pattern. The system will be capable of displaying the number of relationships allowable based on the available memory at run-time on the Retrieve Relationship screen.

When the Supervisor/Librarian selects a relationship to be retrieved, the relationship information will be displayed on the Relationship screen. The Supervisor/Librarian will have the option to cancel this operation.

4.2.2.7.3 Save Relationship. The Supervisor/Librarian will be able to save relationships to the system. The total number of relationships that may be added will be restricted only by the available memory at runtime. The system will enforce uniqueness of the relationships within

the local site catalog. The system will update all the Related RA list entries that include the updated relationship.

4.2.2.7.4 Delete Relationship. The Supervisor/Librarian will be able to delete an existing relationship from the system. The Supervisor/Librarian will be prompted to confirm deletion of the relationship. The system will delete all the related RA list entries that include the deleted relationship.

4.2.2.8 Logs.

4.2.2.8.1 Usage Log. The Supervisor/Librarian will be able to update or delete RA usage log entries with information solicited from local users. A usage log entry will be made when an asset is extracted from the DSRS by a programmer-level user. The usage log will be updated on the system where the asset is physically located and the user's host site. The following information will be displayed for each usage log entry:

a. RA ID,

b. User ID for the user who requested the RA,

c. Site ID for the user who requested the RA,

d. Date the RA was requested,

e. Date the RA was extracted or issued, and

f. Method of extraction.

In the case of a file or FTP extraction, the data of the actual extraction is provided by the system. In the case of the tape or hard copy request, the Supervisor/Librarian manually enters the date issued when the tape or hard copy is sent.

4.2.2.9 Import. The Supervisor/Librarian will be able to specify an export file to be imported into the local repository. The export file must have been created using the DSRS export function using the same version of the DSRS system and will be verified.

All RA information in the specified export file will be read and inserted into or used to update existing information in the repository. The import facility will be a batch process; therefore, the process will not allow for a planned interrupt by the Supervisor/Librarian. The Supervisor/Librarian must specify the pathname and filename of the export file that will be imported. A log containing the status of each transaction will be displayed. Any errors that

occur during the import process will be logged in the log file. The following paragraphs indicate the information that will be imported into the local database:

a. **Group.** The group containing the RAs to import.

b. **Basic RA Information.** Information that will be stored for each RA, including the RA ID, RA version, state, asset long name, UID, timestamp, author flag, point-of-contact ID, date submitted, date updated, and site ID.

c. **Metrics.** The metric type and metric from the export file. If any of the imported RA's metric types do not exist in the local database, then those metric types and metric values will be logged as warnings in the import log file and will not be imported into the local database.

d. **Classification.** The descriptors (domain, facet and facet term) from the export file. If any of the imported RA's descriptors do not exist in the local database, those descriptors will be logged as warnings in the import log file and will not be imported into the local database.

e. **Related RA List.** The related RA IDs and their relationships from the export file. If any related RA ID and its relationship do not exist in the local catalog, that related RA will be logged as a warning in the import log file and will not be imported into the local database.

f. **RA File List.** The list of RA files including the RA file, filename, and file type for each file will be imported (not the contents of the files).

4.2.2.10 Export RAs. The Supervisor/Librarian will be able to create a list of local and remote active RA(s) to be exported. RAs to be exported will be specified by an existing Group ID. The number of RAs that may be exported will be restricted by the available memory at runtime and by available disk space. The Supervisor/Librarian will be able to export RAs to remote DSRS sites and other interoperable repositories.

4.2.2.10.1 Export RAs to Remote DSRS Sites. The Supervisor/Librarian will be able to create an export file that can be imported into remote DSRS sites. Active RAs and associated information to be exported will be written to an export file in a format compatible with the Librarian Import capability. The Supervisor/Librarian will have the capability to create an export file in DSRS format. The Supervisor/Librarian must specify the pathname and filename of the export file. The export file will contain the following information:

a. **Group.** The group containing the RAs to be exported.

b. **Basic RA Information.** Information that will be stored for each RA shall be exported, including the RA ID, RA version, state, asset long name, UID, timestamp, author flag, point-of-contact ID, date submitted, date updated, and site ID.

c. **Metrics.** The type of measure and numeric value.

d. **Classification.** The descriptors (domain, facet, and facet term combinations).

e. **Related RA List.** The related RA IDs and their relationships.

f. **RA File List.** The list of RA files, including the RA file, filename, and file type for each file (not the contents of the files).

4.2.2.10.2 Export RAs to Other Interoperable Repositories. The Supervisor/Librarian will be able to create an index file containing active RAs and associated information to be exported to other interoperable repositories. The index file will be in a format specified in the *ASSET/CARDS/DSRS Library Interoperation* specification. The Supervisor/Librarian must specify the pathname and filename of the index file. The index file will contain the following information for each RA:

a. **Basic RA Information.** Information that will be stored for each RA shall be exported, such as the RA ID, RA version, asset long name, UID, point-of-contact ID, date submitted, and date updated.

b. **Keyword (Descriptor) List.** The descriptors (domain, facet, and facet term).

c. **RA File List.** The list of RA files, including the RA file, filename, and file type for each file (not the contents of the files).

4.2.2.11 Reports. The Supervisor/Librarian will be able to generate reports on the data in the system. These reports will be predefined to reduce the complexity of generating reports. The reports cover historical information from the user's audit information and database content reports.

4.2.2.12 Options.

4.2.2.12.1 Server Options. The Supervisor/Librarian will be able to specify the server's hostname, database name, TCP port, and TCP timeout.

4.2.2.13 Help. The system will provide a Help option on most screens in the tool. This option will provide the capability to view on-line Help in order to assist Supervisor/Librarians in operating the system.

4.2.2.13.1 Contents. The system will provide Supervisors/Librarians with a list of available topics that can be selected to view additional information. The help topics will cover such information as an overview of the system, an explanation of Supervisor/Librarian functions, a description of how to execute the Supervisor/Librarian functions, and restricted functions.

4.2.2.13.2 Search Help. The system will provide help for the current screen, including information for the data fields and valid operations from the current screen.

4.2.2.13.3 Suggestions. The user will be able to enter suggestions and comments at anytime during the operation of the tool. These suggestions will be stored as e-mail messages and will include the user ID, data, subject, and text.

4.2.2.13.4 Tutorial. The system will provide the Supervisor/Librarian with an on-line tutorial. The tutorial will instruct beginners on how to execute basic DSRS Librarian functions.

4.2.2.14 Exit. The system will allow the Supervisor/Librarian to log out of the system and return to the host system environment.

4.2.3 Server. The Server will process requests from the clients.

4.2.3.1 Authentication Requests. The Server will authenticate user login requests. The user's User ID and password will be required. The Server will update the user's last login date upon successful login.

4.2.3.2 Catalog Requests. The server will provide the changes to the requested data type based on the date of the last update requested by the client. The following data types may be requested by the User Tool clients:

a. Domains,
b. RA Classification (Domain, Facet, Facet Term),
c. RA ID and Long Name,
d. RA Metrics,
e. RA File List, and
f. Related RA List.

4.2.3.3 File Transfer Requests. The server will process browse and extract requests. The Server will authenticate the client site, validate the group/site assignments for the requested RA, and maintain the usage log. A user will be able to search and extract an RA if (1) the RA information exists in the user's server database; and (2) the RA is assigned to a group to which the user and the user's site are also assigned. Otherwise, the user will not have access to the RA. In other words, the RA will not be available as a candidate RA; therefore, the RA will not be able to be extracted. For remote RAs: (1) the RA information must be in the user's server database; and (2) the user's site must have been assigned to some group containing the asset at the remote site. For foreign RAs: (1) the RA information must be in the user's server database; and (2) the foreign site must have granted access rights to the user's site (using procedures defined and used at the foreign site). Once the request is validated, the file(s) for the requested RA will be transferred to the client site. Basic error checking and recovery will be supported during the transfer of each file.

4.3 FLEXIBILITY.

a. The DSRS will be independent of organizational structure. DSRS functions will be based on processes rather than on people; therefore, it will be able to easily withstand organizational structure changes. A principal design consideration will be to incorporate functional modularity.

b. The DSRS functional design minimizes dependence on the host environment. The DSRS was designed to accommodate changes in the technical environment. To maximize portability, XVT Development Solution for C++™ (DSC++) will be the User Tool interface. Visual Basic will be used to generate a Windows implementation of the User and Librarian Tool interfaces.

c. The DSRS will be table-driven.

d. The DSRS will be designed to accommodate changes in requirements and/or operating environment. The design allows enhancements and changes in requirements to be incorporated periodically. Because the DSRS will be designed to use relational database technology, changes in structure and data will be more easily accomplished. With this consideration in mind, the system will be designed with a maximum amount of flexibility so as to adapt to future changes quickly and easily.

4.4 SYSTEM DATA. The inputs, outputs, and database description are provided in the *System Specification for the DSRS* and the *Database Specification for the DSRS*.

SECTION 5
ENVIRONMENT

5.1 EQUIPMENT ENVIRONMENT.

5.1.1 DSRS Server. The DSRS Server will require the following equipment configuration:

a. Sun 4 architecture

b. 300 MB minimum available disk storage

c. Tape Backup Device (available within network)

d. CD - ROM

e. Ethernet connection to the DDN/Internet

f. Modems (based on the number of users dialing in)

g. 16 MB of memory (minimum).

The system configuration listed above should be considered the minimum configuration. The actual CPU size, disk storage, and memory requirements will vary according to the number of users, number and size of the RAs, and RA information in the system. The disk storage specified includes: DSRS executables, configuration files, utility files, unit and system test files, and source files. This disk storage may be computed by multiplying the expected number of RAs by the average size of an RA.

5.1.2 DSRS Client for MS-Windows. The DSRS User for Windows and the DSRS Librarian for Windows will require the following equipment configuration:

a. 386/486/Pentium IBM PC Compatible 25 MHz (or higher), 486/Pentium IBM PC compatible 50 MHz (or higher) for the Librarian Tool

b. 8 MB memory (minimum)

c. 5 MB available hard disk space (minimum)

d. 3 1/2" 1.44 MB Floppy Disk Drive or 5 1/4" 1.2 MB Floppy Disk Drive

e. Ethernet interface adapter or 9600 Baud MODEM (or higher) for PPP/SLIP

f. CD - ROM Drive (optional)

g. Sound adapter with speakers (optional).

5.1.3 DSRS Client for UNIX. The DSRS client for UNIX will require the following equipment configuration.

a. Sun 4 architecture

b. 10 MB minimum available disk storage

c. 16 MB memory (minimum)

5.2 SUPPORT SOFTWARE ENVIRONMENT.

5.2.1 SunOS 4.1.3 Environment.

5.2.1.1 DSRS Server. Support software for the DSRS Server running on the Sun system is shown in Table 5-I.

Table 5-I. Support Software for the DSRS Server

Software	Runtime Environment	Development Environment
SunOS Version 4.1.3 (Solaris 1.1)	•	
ORACLE7 Server Release 7.1.3.0.0	•	
ORACLE SQL*Plus Release 3.1.3.4.1	•	
ORACLE SQL*Net for TCP/IP Version 1.0	•	
ORACLE PL/SQL Release 2.1.3.0.0.0	•	
GNU ANSI C Compiler 2.3.3		•
ORACLE Pro*C Release 1.6.4.0.0		•

5.2.1.2 DSRS for X/Motif. The support software for the DSRS X/Motif is shown in Table 5-II.

Table 5-II. Support Software for the DSRS for X/Motif

Software	Runtime Environment	Development Environment
SunOS Version 4.1.3 (Solaris 1.1)	•	
Open Windows Version 3.0	•	
ICS OSF Motif Version 1.2.4	•	
ICS OSF Motif Version 1.2.2		•
Minerva MSQL RDBMS Version 1.0	•	
XVT-Power++ 3.0		•
SPARCworks Professional C++, SPARCworks 3.0.1		•
SPARCompiler C++ 4.0.1		•
GNU ANSI C Compiler 2.3.3		•
XVT-Graphical Extensions 2.0		•

5.2.2 Solaris 2.3 Environment.

5.2.2.1 DSRS Server. Support software for the DSRS Server running on the Sun system is shown in Table 5-III.

Table 5-III. Support Software for the DSRS Server

Software	Runtime Environment	Development Environment
SunOS Version 5.3 (Solaris 2.3)	•	
ORACLE7 Server Release 7.1.3.0.0	•	
ORACLE SQL*Plus Release 3.1.3.4.1	•	
ORACLE SQL*Net for TCP/IP Version 1.0	•	

Software	Runtime Environment	Development Environment
ORACLE PL/SQL Release 2.1.3.0.0.0	•	
SPARCworks-Pro-C 3.0.1		•
ORACLE Pro*C Release 1.6.4.0.0		•

5.2.2.2 DSRS for X/Motif. The support software for the DSRS X/Motif is shown in Table 5-IV.

Table 5-IV. Support Software for the DSRS for X/Motif

Software	Runtime Environment	Development Environment
SunOS Version 5.3 (Solaris 2.3)	•	
Open Windows Version 3.3	•	
ICS OSF Motif Version 1.2.2	•	•
Minerva MSQL RDBMS V1.0	•	•
XVT-Power++ 3.0		•
SPARCworks Professional C++, SPARCworks 3.0.1		•
SPARCompiler C++ 4.0.1		•
SPARCworks-Pro-C 3.0.1		•
XVT-Graphical Extensions 2.0		•

5.2.3 MS-Windows Environment.

5.2.3.1 DSRS for Windows. The support software for the DSRS for Windows is shown in Table 5-V.

Table 5-V. Support Software for the DSRS for Windows

Software	Runtime Environment	Development Environment
Microsoft DOS Version 5.0 (or higher)	•	
Microsoft Windows Version 3.1	•	
Trumpet Winsock 2.1	•	
Microsoft Visual Basic Version 3.0		•
Microsoft Access Version 1.1		•
Desaware CCF - Cursors Version 2.0		•
Desaware Custom Control Factory		•

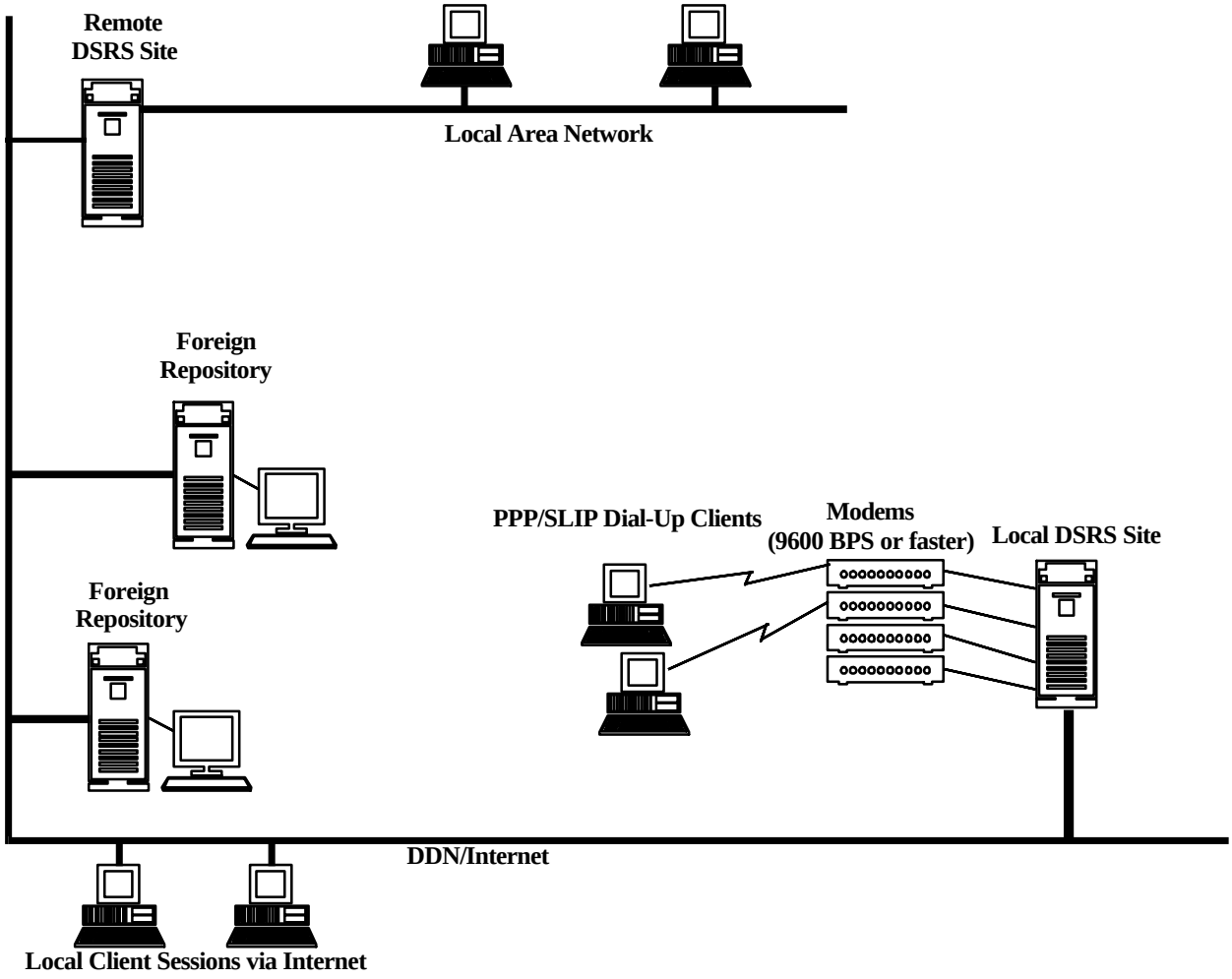
Version 2.0		
NetManage NEWT-SDK Version 3.11 Blue Sky RoboHelp Version 3.0		• •

5.2.3.2 DSRS Librarian for Windows. The support software for the DSRS Librarian for Windows is shown in Table 5-VI.

Table 5-VI. Support Software for the DSRS Librarian for Windows

Software	Runtime Environment	Development Environment
Microsoft DOS Version 5.0 (or higher)	•	
Microsoft Windows Version 3.1	•	
ORACLE SQL*Net TCP/IP Version 1.1 for Windows	•	
Trumpet Winsock 2.1	•	
Microsoft Visual Basic Version 3.0		•
Desaware CCF - Cursors Version 2.0		•
Desaware Custom Control Factory Version 2.0		•
NetManage NEWT-SDK Version 3.11		•
Borland ReportSmith Version 2.3		•
Blue Sky RoboHelp Version 3.0		•

5.3 COMMUNICATIONS REQUIREMENTS. The communications path between remote sites will take place over DDN/Internet for the UNIX system. Communications over DDN will be supported via TCP/IP Sockets. Dial-in users will require terminal emulation communications software that supports SLIP or PPP. The medium for dial-up terminals is a modem with voice-grade telephone lines.



5.3.1 Graphic Overview. The hardware and software environment will conform to the above listed minimum requirements. A graphical overview of the DSRS communications paths is displayed in Figure 5-1.

Figure 5-1. DSRS Communications Overview

5.3.2 Hardware. DSRS site computers require appropriate Internet connections to be able to perform remote extractions. This may include Ethernet hardware, routers, and appropriate assignment of Internet addresses.

5.3.3 Software. Software operating on hardware systems described in Section 5.1 will conform to the requirements identified in the previous sections. Users may use various TCP/IP software packages to access the DSRS. Network connections to the Internet will require appropriate Transmission Control Protocol/Internet Protocol (TCP/IP) networking software.

5.3.4 Modems. A modem may be used from a PC to connect to the MS-Windows User Tool. Using a modem to connect to the DSRS requires hardware and software to be installed on the calling end and on the server which is the receiving end. The user needs a recommended minimum 9600 bps modem installed on the calling PC. The TCP/IP software on the user's PC needs a PPP/SLIP option. The server needs a recommended minimum 9600 BPX modem for users to establish a PPP/SLIP connection with a modem. The TCP/IP software on the server needs a PPP/SLIP option. With the various TCP/IP software available, no specific vendors are recommended.

Using the modem to connect to the server allows the PC access to the DSRS and the Internet. Access to the Internet is required for proper operation of the DSRS. The PPP/SLIP connection to the server creates the TCP/IP stack necessary for Internet communication.

5.4 INTERFACES. The communication architecture is illustrated in Figure 5-1.

5.4.1 TCP/IP Asset Transfer Interface. The DSRS component transfer is an interaction between two sites (DSRS or foreign) via an application layer protocol transported via TCP/IP. The protocol implements a client/server architecture in which the local DSRS User Tool becomes a client to the Interoperability Server of an owning site. The Interoperability component transfer protocol will provide the basic set of operations for gathering data, transmitting it, and using it properly on the receiving site. This protocol will operate over the Internet and/or local TCP/IP networks. Remote extraction is automated by the DSRS User Tool through the use of the extract command. A user's extract request for remote RAs generates a client transaction to the cooperating site's server; the local DSRS User Tool will communicate with the cooperating site's server. The Interoperability Server located at the remote site will process extract requests and transmit components and extract status to the client.

5.4.2 DSRS-to-ORACLE Interface. Since DSRS uses ORACLE as its underlying database, a communications interface exists between them. The DSRS communicates with ORACLE

using SQL and the ORACLE database interface. This communication is local to one computer system; i.e., the DSRS and ORACLE will execute on the same platform.

5.4.3 User Terminal Interface. Users will connect with the DSRS using PPP/SLIP dial-up MS- Windows connections, sessions over the Internet, or X sessions over the Internet. The interface between the user's terminal and the DSRS is provided in large part by the underlying operating system and networking software. X sessions may be executed over a TCP/IP network such as the Internet.

5.5 SUMMARY OF IMPACTS. The DSRS will be operational in a normal office environment with suitable office equipment (air conditioning, sound muffling devices for printers, etc.) available for the hardware. The system will not require the support of an ADP organization beyond the requirement for communications support. Therefore, the system is not anticipated to result in a significant organizational, operational, or developmental impact.

5.6 FAILURE CONTINGENCIES. It is anticipated that hardware and software failures may occur as the DSRS is being deployed. It is also anticipated that failure may occur at some installations after field testing is completed. Minor problems will occur during the initial phases of learning the system by the DSRS System Administrator. The answer to such problems will, at least partly, be found in the documentation and learned through training. Every effort will be made to ensure that documentation and embedded help screens are clearly written and helpful to the user in solving minor, routine system problems.

5.6.1 Restart/Recovery due to Loss of Database. Frequency of backups will depend on local policy and the operational environment. The system is a stand-alone system requiring no restart procedures within the application software. The relational DBMS must support automatic roll back of all partially completed transactions due to hardware or software failures. Users performing data manipulation operations at the time of a failure will be required to check the last activity on which they were working. This activity may have to be repeated.

5.6.2 Restart/Recovery due to Software Errors. Problems due to application software errors will be reported to the SRP for resolution. Refer to the *System Administration Manual for the DSRS* for additional information.

5.7 ASSUMPTIONS AND CONSTRAINTS.

a. **Hardware, Software and Communication Environment.** The host site will provide and maintain the environment as described in Sections 5.1, 5.2, and 5.3 of this document.

b. **Manpower.** The manpower required to operate and maintain the system will be provided by the using organization.

SECTION 6
SECURITY

6.1 BACKGROUND INFORMATION. The DSRS is a non-mission critical system. Its primary purpose is to facilitate the potential for cost savings by providing a repository for reusable software. As a result, potential threats to the DSRS can be grouped primarily into the area of data integrity. While confidentiality is a concern, the greatest challenge facing SRP personnel is maintaining the integrity of software objects being reused. The security controls and mechanisms of the DSRS are provided by the operating system, the DSRS application itself, and administrative procedures established by the SRP personnel.

6.1.1 System Security Requirements. Guidance for determining the security requirements for DOD Automated Information Systems (AISs) is provided in DOD Directive 5200.28, *Security Requirements for Automated Data Processing (ADP) Systems* and DOD Directive 5200.1-R, *Information Security Program Regulation*. These policies require all DOD activities to implement a cost-effective AIS Security Program to protect AISs against unauthorized disclosure, modification, destruction, and denial of service. Specific security implementations are contained in the *DSRS Security Plan*, the *DSRS Trusted Facility Manual*, the *Security Feature Users Guide* and the SRP Standing Operating Procedures (SOP). The major goal of the DSRS Security Program is to have the system and network operating at an acceptable level of risk for the Designated Approving Authority (DAA) to grant accreditation. The DAA provided formal implementation of the DSRS on 17 July 1995. To ensure that the DSRS continues to operate at an acceptable level of risk, the DSRS Security Program has established the following objectives:

a. Maintain a high level of confidentiality to prevent unauthorized access to proprietary information;

b. Prevent the misuse of Government computer resources;

c. Protect information from unauthorized modification, which could cause harm to the DSRS, or more importantly, user systems; and

d. Ensure the availability of information to meet customer requirements.

6.1.2 C2 Security Requirements. The computer security requirements for the DSRS were determined by identifying the security operating mode and applying the evaluation criteria presented in CSC-STD-004-85, *Guidance for Applying the Department of Defense Trusted*

Computer Evaluation Criteria in Specific Environments. The DSRS currently operates in System High mode, which is defined as a system in which all system users possess clearance and authorization for all information contained in the system. Additionally, DOD Directive 5200.28 requires that all computer resources that process or handle Classified or Sensitive Unclassified information implement at least C2 functionality (Controlled Access Protection) by calendar year 1992.

6.1.3 C2 Security Requirements Overview. Systems in this class are required to enforce a more finely grained, discretionary access control than C1 systems, making users individually accountable for their actions through login procedures, auditing of security-relevant events, and resource isolation. The specific requirements for class C2 protection are provided below with a brief description of each requirement.

a. **Discretionary Access Control.** Restrict access to objects (e.g., files) based on the identity of individuals or defined groups of individuals to protect objects from unauthorized access and to limit propagation of access rights. The controls are discretionary in the sense that owners of data, at their discretion, are capable of permitting others to access data.

b. **Object Reuse.** Eliminate all residual data from a medium (e.g., disk sector) before reassignment of that medium from one subject to another. This prevents users with utility programs from scanning the medium and recovering residual data.

c. **Identification and Authentication.** Identify each individual user of an AIS system before user activity on that AIS system. Establish protective mechanisms, such as passwords, to authenticate the user's identity and to associate all auditable actions taken by that user.

d. **Audit.** Create and maintain an audit trail so that all actions affecting the security of an AIS system can be traced to the responsible party based on individual identity. The AIS system must protect the audit information from modification or unauthorized access or destruction by an unauthorized individual. At a minimum, the following events will be provided by the audit mechanism:

(1) Use of identification and authentication mechanisms;
(2) Introduction of objects into the user's address space;
(3) Deletion of objects from a user's address space;
(4) Actions taken by Computer Operators, System Administrators, and Security Personnel;

(5) All security-relevant events; and
(6) Production of printed output.

The following information is required to be documented by the audit trail:

(1) Date and time of the event;
(2) The unique identifier on whose behalf the subject generating the event was operating;
(3) Type of event;
(4) Success or failure of the event;
(5) Origin of the request (e.g., terminal ID) for identification and authentication events;
(6) Name of object introduced, accessed, or deleted from a user's address space; and
(7) Description of modifications made by the System Administrator to the user/system security databases.

e. **System Architecture.** Create and maintain a domain for execution to protect the Trusted Computing Base (TCB) from external interference or tampering. The TCB shall isolate the resources to be protected so that they are subject to the access control and auditing requirements.

f. **System Integrity.** Provide hardware and software features that will validate correct operation of hardware and firmware elements of the TCB.

g. **Security Testing.** Test security protection mechanisms to confirm their working order as claimed in the system documentation, so that obvious flaws shall be properly identified and corrected.

h. **Security Features Users Guide.** Prepare a section in the user documentation describing the protection mechanisms provided by the TCB, guidelines on their use, and how they interact with one another.

i. **Trusted Facility Manual.** Prepare documentation addressing the functions and privileges needing to be controlled when running a secure facility, as well as procedures for examining and maintaining audit files and a detailed audit record structure for each type of audit.

j. **Security Testing Documentation.** Prepare documentation that describes the test plan and results of the security mechanism's functional testing.

k. **Security Design Documentation.** Make available manufacturer's documentation that describes their philosophy of protection and how it relates to the TCB. This document should also include the description of the interfaces between these modules.

6.2 CONTROL POINTS, VULNERABILITIES AND SAFEGUARDS. This section describes each control point, the vulnerabilities at the control point, and the safeguard requirements to reduce the risk to an acceptable level. This description includes consideration of alternate modes of operation based on emergency, disaster, or accident, when appropriate.

6.2.1 Control Points. A control point can be located at any interface where there is movement of data within or between sites. The following control points are considered for this application: input, process, and output.

6.2.1.1 Input Control Points.

6.2.1.1.1 Origin. Data origination controls are used to ensure the accuracy, completeness, and timeliness of data before they are converted into a machine-readable format and entered into the computer application data tables. Controls should ensure that the data reach the application without loss, unauthorized addition, modification, or error. Controls over the data should be established as close to the point of origination as possible, as the remainder of the application processing depends on the accuracy of the source data.

Modification of system edits, required entries, and audit rules should be inaccessible to all users except the local System and Security Administrators.

6.2.1.1.2 System Access/Data Entry. Data input controls ensure the accuracy, completeness, and timeliness of data during their conversion into machine-readable format and entry into the application data tables. The DSRS is unique in that programmer-level users do not directly enter data into the system. Each asset entered into the system is assigned a certification level, which identifies the thoroughness of review by certification personnel. All data entry into the system is accomplished by an authorized Supervisor/Librarian.

a. Password controls should be used to prevent unauthorized access to the system.

b. When keying passwords and authorization codes, non-printing and non-displaying facilities should be used.

c. User access will be disabled, modified, or deleted, as applicable.

d. Documented procedures should be developed to explain the process of identifying, correcting, and reprocessing data rejected by the application.

e. No person should be able to bypass the validation process.

f. Data validation and editing should be performed as early as possible in the data flow to ensure that the application rejects any incorrect transaction before its entry into the data tables.

6.2.1.1.3 Error Correction. Data input errors will be detected and corrected on the data input menu-driven screen.

a. All data entered into the DSRS must be validated at the source of entry. Each data field on the input screen will be subjected to edits that will include alphabetic, alphanumeric, numeric, and verification against tables, ranges, and values, as appropriate.

b. When invalid input is detected, a screen notification and error identification will be displayed on the workstation.

6.2.1.2 Process Control Points. Process controls are procedures designed to streamline transactions to reduce data errors.

6.2.1.2.1 Accuracy and Completeness. The DSRS module will notify the user of the processing success/failure in an on-line message for interactive input.

6.2.1.2.2 System Interfaces. The DSRS interfaces are described in detail in Section 5.4. None of the systems involved are classified. It is assumed that data accepted from other systems will have been through validity edits.

6.2.1.3 Output Control Points. Output control points are the final areas where data accuracy can be monitored. Two output control points occur; they are discussed in the following subparagraphs.

6.2.1.3.1 Production. Production devices authorized to receive output will be determined by the user's access rights. Output devices may be located within a local area network and will consist of various models of both networked printers and local printers. Output will also be provided to exportable magnetic media such as floppy diskette or tape.

6.2.1.3.2 Distribution. The application will distribute output products as an on-line response to a process. Other forms of distribution will be by hard-copy listing or by electronic

distribution; both will be generated by the DSRS Librarian after validating receipt of an extract request.

6.2.2 Vulnerabilities. The input of the DSRS application is vulnerable to erroneous input, modification, or deletion of data. Vulnerabilities are discussed by the categories' input control points, processing control points, and output control points.

6.2.2.1 Input Control Points. Vulnerability to unauthorized input, modification, or deletion of data will be controlled by the user's access rights.

a. **Origin**. Vulnerabilities at the point of origin include erroneous information in the input data.

b. **Data Entry**. Librarian error is a vulnerability at this point. Erroneous keystrokes, incomplete information, or other entry errors are types of vulnerabilities encountered.

c. **Disposition**. The loss of source documents prior to verification and correction would have an adverse impact on the accuracy of the application.

d. **Error Correction**. Verification of the accuracy of data used in the correction of input data is required. Although validity edits will be used whenever possible, input of some data is still vulnerable to data entry errors.

6.2.2.2 Processing Control Points. Two processing control points are examined.

a. **Accuracy and Completeness**. One of the critical factors in the effective operation of the application is complete and accurate input data. There must be on-line messages to inform the operator of the success or failure of entering data.

b. **System Interfaces**. Interfaces with other systems have three vulnerabilities:

(1) Potential for processing errors or incorrect data being added to the application,
(2) Possibility of errors being introduced during the transfer process, and
(3) Receiving or target system does not receive the entire input data or the data received are not accurate.

6.2.2.3 Output Control Points. One of the vulnerabilities of a networked configuration is that data could be routed to an unauthorized user. This vulnerability could result in the disclosure of proprietary information to an unauthorized user.

6.2.3 Safeguards. A safeguard is a requirement that will reduce the vulnerabilities at each control point. This section discusses the precautions that can be taken to manage the system vulnerabilities previously described. These include administrative, physical, and technical safeguards.

6.2.3.1 Administrative Safeguards. An administrative safeguard is defined as any procedure that requires management supervision.

6.2.3.1.1 Personnel. Currently, DSRS contains only Unclassified but Sensitive data and, therefore, no security clearance is required for users of the system. Authorization to perform specific functions will be controlled through the user's access rights.

6.2.3.1.2 Collection and Preparation. All data entered into the DSRS will be edited at the source of entry and will be validated against tables, ranges, and values. When invalid input is detected, a screen notification and error identification will be displayed on the workstation.

6.2.3.1.3 Environment Constraints. To provide the assurance that the system will be protected from unauthorized access, the System Administrator will set normal working hours for each user on the system during the process of issuing the new User ID, password, and privileges. These restrictions will be enforced by the system at all times. The System Administrator will also designate a time during non-peak hours that users will not be allowed access to the system, so that backup and maintenance procedures can be accomplished. This will also apply to stand-alone systems. Users will also be required to complete an Account Request Form with a program manager's signature and Non-Disclosure Statement before being issued an account.

6.2.3.2 Physical Safeguards. DODD 5200.28 requires that personnel responsible for Sensitive Unclassified AISs protect hardware, software, documentation, and data from unauthorized disclosure, destruction or modification. Protective means can include personnel, physical, administrative, and configuration controls.

6.2.3.3 Technical Safeguards. Three technical safeguards are examined: user access, process safeguards, and multilevel security requirements.

6.2.3.3.1 User Access. The user must complete an Account Request Form (ARF), which must then be approved by a program manager. The ARF will help control access to the library by requiring authorization of the program manager. Once the ARF is processed, the

user will receive a User ID and password. Access to a library system will also be controlled by User ID and password assigned to the user. The user will log in using the User ID followed by the password. If the user does not respond with the correct User ID and password within three attempts, the system will lock the account and require administrator action to reset. Additionally, the server will automatically log off a user after 10 minutes of inactivity. The Librarian will have the ability to assign/deny functional access based on the User ID. The functionality, along with the privileges, will completely define the user's access privileges within a system. It is the responsibility of each DSRS site to establish procedures for processing user accounts.

6.2.3.3.2 Process Safeguards. Whenever feasible, all data entered will be edited at the source of entry and verified against tables, ranges, and values. When invalid input is detected, a screen notification and error identification will be displayed on the workstation.

6.2.3.3.3 Multilevel Security Requirements. The DSRS currently contains only Unclassified but Sensitive (UBS) assets and, as such, there is no requirement for automatic security labeling of subjects (users) and objects (data) in the system.

6.3 SYSTEM MONITORING AND AUDITING. The audit requirements have been identified in paragraph 6.1.3.d and are detailed in the *DSRS Security Plan* and *DSRS Trusted Facility Manual*. The system will provide an audit trail to track system usage and access to RAs on the system. In addition, individual user sessions will generate an audit trail that can be reviewed for errors (i.e., Server log entries).

DSRS TRACEABILITY MATRIX

Functional Description	System Specification	Database Specification	Computer Operation Manual	Maintenance Manual	Librarian Manual	U Ma
4.2.1.1	4.2.1.a, 4.4.1	4.1.3, 4.1.5	2.2.1, 3.5, 3.6	5.1, 2.1.1.1		4.2.1, 5.2.1
4.2.1.1.2	4.2.1.a.1, 4.4.1.1	4.1.3, 4.1.5	2.2.1, 3.5, 3.6	5.1, 2.1.1.1.2		4.2.1, 5.2.1
4.2.1.1.4	4.2.1.a.2, 4.4.1.2	4.1.3, 4.1.5	2.2.1, 3.5, 3.6	5.1, 5.2, 5.7		4.2.1.1, 5.2
4.2.1.2	4.2.1.b, 4.4.7.1	4.1.1, 4.1.2, 4.1.3	2.2.1, 3.5, 3.6	5.1, 5.8, 2.1.1.2		4.2.2, 5.2.2
4.2.1.3	4.2.1.c, 4.4.2	4.1.1	2.2.1, 3.5, 3.6	5.1, 5.3, 2.1.1.3		4.2.3, 5.2.3
4.2.1.4	4.2.1.d, 4.4.3	4.1.1	2.2.1, 3.5, 3.6	5.1, 5.4, 2.1.1.4		4.2.4, 5.2.4
4.2.1.5	4.2.1.e, 4.4.4	4.1.1, 4.1.2, 4.1.4, 4.1.5, 4.1.6, 4.1.7	2.2.1, 3.5, 3.6	5.1, 5.5, 5.7, 2.1.1.5		4.2.5, 5.2.5
4.2.1.6	4.2.1.f, 4.4.5	4.1.4	2.2.1, 3.5, 3.6	5.1, 5.6, 2.1.1.6		4.2.6, 5.2.6
4.2.1.7.2	4.2.1.g, 4.4.13	4.1.4	2.2.1, 3.5, 3.6	5.1, 2.1.1.7.2		4.2.7.2, 5.2
4.2.1.8	4.2.1.g, 4.4.13		2.2.1, 3.5, 3.6	5.1, 2.1.1.8		4.2.8, 5.2.8
4.2.2.1.1.1	4.2.2.1.a, 4.4.7	4.1.1, 4.1.2, 4.1.8	2.2.2, 3.7	5.1, 5.8, 5.9, 2.1.2.1.1.1	4.3.1.1	
4.2.2.1.1.2	4.2.2.1.a, 4.4.7	4.1.1, 4.1.2, 4.1.8	2.2.2, 3.7	5.1, 5.8, 2.1.2.1.1.2	4.3.1.2	
4.2.2.1.2.1	4.2.2.1.b.1, 4.4.8.1	4.1.3	2.2.2, 3.7	5.1, 5.10, 2.1.2.1.2.1	4.3.2.1, 4.3.2.2	
4.2.2.1.2.2	4.2.2.1.b.2, 4.4.8.2	4.1.3	2.2.2, 3.7	5.1, 5.11, 2.1.2.1.2.2	4.3.2.3	
4.2.2.1.3	4.2.2.1.d, 4.4.9.2	4.1.4, 4.1.6	2.2.2, 3.7	5.1, 5.13, 2.1.2.1.3	4.3.3	
4.2.2.1.4	4.2.2.1.c, 4.4.9.1	4.1.6	2.2.2, 3.7	5.1, 5.12, 2.1.2.1.4	4.3.4	
4.2.2.1.5	4.2.2.1.f, 4.4.11	4.1.4	2.2.2, 3.7	5.1, 5.15, 2.1.2.1.5	4.3.5	
4.2.2.1.6	4.2.2.1.e, 4.4.10	4.1.4	2.2.2, 3.7	5.1, 5.14, 2.1.2.16	4.3.6	
4.2.2.1.7.2	4.2.2.1.g, 4.4.13	4.1.4	2.2.2, 3.7	5.1, 2.1.2.1.7.2	4.3.7.2	
4.2.2.1.8	4.2.2.1.g, 4.4.13		2.2.2, 3.7	5.1, 2.1.2.1.8	4.3.8	
4.2.2.2.1	4.2.2.2, 4.4.12.1	4.1.1, 4.1.8	2.2.3, 3.8	5.17, 2.1.2.2.1	5.3.1	
4.2.2.2.2	4.2.2.2, 4.4.12.1	4.1.5	2.2.3, 3.8	5.17, 2.1.2.2.2	5.3.2	
4.2.2.2.3	4.2.2.2, 4.4.12.1	4.1.1, 4.1.2, 4.1.8	2.2.3, 3.8	5.17, 2.1.2.2.3	5.3.3	
4.2.2.2.4	4.2.2.2, 4.4.12.1	4.1.4	2.2.3, 3.8	5.17, 2.1.2.2.4	5.3.4	
4.2.2.2.5	4.2.2.2, 4.4.12.1	4.1.1	2.2.3, 3.8	5.17, 2.1.2.2.5	5.3.5	
4.2.2.2.6	4.2.2.2, 4.4.12.1	4.1.4	2.2.3, 3.8	5.17, 2.1.2.2.6	5.3.6	

Functional Description	System Specification	Database Specification	Computer Operation Manual	Maintenance Manual	Librarian Manual	U Ma
4.2.2.2.7	4.2.2.2, 4.4.12.1	4.1.4	2.2.3, 3.8	5.17, 2.1.2.2.7	5.3.7	
4.2.2.2.8	4.2.2.2, 4.4.12.1	4.1.3	2.2.3, 3.8	5.17, 2.1.2.2.8	5.3.8	
4.2.2.2.9	4.2.2.2, 4.4.12.1	4.1.6	2.2.3, 3.8	5.17, 2.1.2.2.9	5.3.9	
4.2.2.2.10	4.2.2.2, 4.4.12.1	4.1.6	2.2.3, 3.8	5.17, 2.1.2.2.10	5.3.10	
4.2.2.3.1	4.2.2.3, 4.4.12.2	4.1.4	2.2.4, 3.9	5.16, 2.1.2.3.1	6.3.1	
4.2.2.3.2	4.2.2.3, 4.4.12.2	4.1.1	2.2.4, 3.9	5.16, 2.1.2.3.2	6.3.2	
4.2.2.3.3	4.2.2.3, 4.4.12.2	4.1.5	2.2.4, 3.9	5.16, 2.1.2.3.3	6.3.3	
4.2.2.3.4	4.2.2.3, 4.4.12.2	4.1.2	2.2.4, 3.9	5.16, 2.1.2.3.4	6.3.4	
4.2.2.3.5	4.2.2.3, 4.4.12.2	4.1.1	2.2.4, 3.9	5.16, 2.1.2.3.5	6.3.5	
4.2.2.4	4.2.2.4, 4.4.12.3	4.1.1, 4.1.2	2.2.5, 3.10	5.18, 2.1.2.3.6	7	
4.2.3.1	4.2.2.5, 4.4.14	4.1.8	2.2.6, 3.11	2.1.3.1, 5.19, 5.7	8.3	
4.2.3.2	4.2.2.5, 4.4.14	4.1.1, 4.1.2, 4.1.8	2.2.6, 3.11	2.1.3.2, 5.19, 5.7	8.3	